NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A FIREWALL TRAINING PROGRAM BASED ON CYBERCIEGE

by

Nai Kwan Tan

December 2005

Thesis Advisor:	Cynthia E. Irvine
Co-Advisor:	Paul C. Clark
Second Reader:	Mike Thompson

THIS PAGE INTENTIONALLY LEFT BLANK

<table>
<tr><td colspan="3">REPORT DOCUMENTATION PAGE</td><td colspan="2">Form Approved OMB No. 0704-0188</td></tr>
<tr><td colspan="5">Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.</td></tr>
<tr><td>1. AGENCY USE ONLY (Leave blank)</td><td>2. REPORT DATE
December 2005</td><td colspan="3">3. REPORT TYPE AND DATES COVERED
Master’s Thesis</td></tr>
<tr><td colspan="3">4. TITLE AND SUBTITLE: A Firewall Training Program Based On CyberCIEGE
6. AUTHOR(S) Nai Kwan Tan</td><td colspan="2">5. FUNDING NUMBERS</td></tr>
<tr><td colspan="3">7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000</td><td colspan="2">8. PERFORMING ORGANIZATION REPORT NUMBER</td></tr>
<tr><td colspan="3">9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A</td><td colspan="2">10. SPONSORING/MONITORING AGENCY REPORT NUMBER</td></tr>
<tr><td colspan="5">11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.</td></tr>
<tr><td colspan="3">12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited</td><td colspan="2">12b. DISTRIBUTION CODE</td></tr>
<tr><td colspan="5">13. ABSTRACT (maximum 200 words)
Firewalls represent an essential tool in networking environments. They are commonly used as an intermediate system to protect an internal network from external networks. It can be destructive to an organization if its sensitive information falls into wrong hands or becomes corrupted. The vulnerability becomes greater if an organization actively uses the Internet. Firewalls play an important role as a first line of defense for the protection of sensitive information and personnel need to understand the proper use of firewall technology and the fundamentals of the packet filtering concepts. Through “hands-on” activities, trainees can experience different types of network attacks and can learn how firewalls can mitigate them.

The goal of this project was to identify the potential capabilities of CyberCIEGE, a simulation created as an interactive educational tool, to help re-enforce packet filtering concepts through the use of computer gaming techniques.

This thesis resulted in refinements to the CyberCIEGE packet filter component to more closely model real- world devices. Scenarios were developed to cover the concepts of packet filtering, filtering against IP spoofing threats and firewalls in demilitarized zone. These refinements and the thesis scenarios contributed to the educational objectives of the tool and benefit the Department of Defense.</td></tr>
<tr><td colspan="4" rowspan="2">14. SUBJECT TERMS Packet Filtering, Firewall, Information Assurance</td><td>15. NUMBER OF PAGES
126</td></tr>
<tr><td>16. PRICE CODE</td></tr>
<tr><td>17. SECURITY CLASSIFICATION OF REPORT
Unclassified</td><td>18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified</td><td colspan="2">19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified</td><td>20. LIMITATION OF ABSTRACT
UL</td></tr>
</table>

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

A FIREWALL TRAINING PROGRAM BASED ON CYBERCIEGE

Nai Kwan Tan
Civilian, Singapore
B.Engg. (Hons), University of Aberdeen, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2005

Author: Nai Kwan, Tan

Approved by: Cynthia Irvine
Thesis Advisor

Paul C. Clark
Co-Advisor

Mike Thompson
Second Reader

Peter Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Firewalls represent an essential tool in networking environments. They are commonly used as an intermediate system to protect an internal network from external networks. It can be destructive to an organization if its sensitive information falls into wrong hands or becomes corrupted. The vulnerability becomes greater if an organization actively uses the Internet. Firewalls play an important role as a first line of defense for the protection of sensitive information and personnel need to understand the proper use of firewall technology and the fundamentals of the packet filtering concepts. Through "hands-on" activities, trainees can experience different types of network attacks and can learn how firewalls can mitigate them.

The goal of this project was to identify the potential capabilities of CyberCIEGE, a simulation created as an interactive educational tool, to help re-enforce packet filtering concepts through the use of computer gaming techniques.

This thesis resulted in refinements to the CyberCIEGE packet filter component to more closely model real-world devices. Scenarios were developed to cover the concepts of packet filtering, filtering against IP spoofing threats and firewalls in a demilitarized zone. These refinements and the thesis scenarios contributed to the educational objectives of the tool and benefit the Department of Defense.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

ACKNOWLEDGMENTS

I would like to express thanks to Prof. Cynthia Irvine, Paul Clark, JD Fulp and Mike Thompson for their inspiring and invaluable guidance during the course of this thesis. Thank you for your patience and constructive critique.

I would like to extend special thanks to Chua Chay and Chee Mun who have influenced and assisted me during the development of this thesis. Your help and friendship has provided me with a unique experience and a great time at Naval Postgraduate School (NPS).

I would like to thank my wife, Edna, for your understanding and unwavering support, through many long hours of work at school and at home.

I also wish to thank my sponsor, Singapore Technologies Engineering (ST Engg.) for the scholarship to participate in this enriching joint program between National University of Singapore and NPS. It has been a wonderful experience to be exposed to American culture.

I would also like to thank Jean Brennan for the kind, excellent and professional support you provide me as a student during my academic at NPS.

Finally, I would also like to thank Steve Cyncewicz for his patient and professional support in editing my thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THESIS STATEMENT

The purpose of this thesis was to explore how CyberCIEGE can be used to develop a gaming environment for firewall topics. The intention was to create educational value and, at the same time, entertainment for trainees on the subject of information security concerning firewalls.

B. CYBERCIEGE

Computer games today are a fast-growing worldwide industry. They are no longer restricted to the entertainment industry as they have penetrated the business and defense markets. Usually, computer games can engage or attract the attention of people for long periods as players tend to play the same game over and over again. This can be used as a means for incorporating educational, learning and training materials.

One area that computer games could be used is to train and educate players about information assurance concepts.

> CyberCIEGE is an ongoing project developed by the Center for Information Systems Security Studies and Research at the Naval Postgraduate School and Rivermind, Inc. The objective of CyberCIEGE is to teach Information Assurance (IA) concepts and practice through gaming. [1]

Training through gaming is an economical and time efficient way to gain the knowledge required for the effective management of information security. Through a simulated "hands-on" approach, trainees can quickly grasp the essential features of technical computer security concepts, such as packet filtering firewalls, management techniques, and other effective ways to protect their networks.

Taking advantage of the popularity of gaming, this thesis makes use of CyberCIEGE to investigate how CyberCIEGE can be used as an effective platform to impart a knowledge of firewall functionality and capabilities. Several questions were raised:

1. What are the differences between the firewall components in the CyberCIEGE game and those of the real world?
2. What changes could be made to the firewall component in CyberCIEGE to more accurately reflect the real world?
3. Can the improved CyberCIEGE firewall components be used to create scenarios that will teach people about firewalls?

A basic understanding of firewalls is required to address the above questions. Addressing these questions enables the design of CyberCIEGE scenarios to effectively illustrate firewall properties within an IA educational laboratory.

C. THESIS SCOPE

The main focus of this thesis research was the development of three CyberCIEGE scenarios that educate the player about firewall functionality. A secondary focus of this thesis research was the refinement of the CyberCIEGE game engine's firewall/router component. Currently, the firewall component in the CyberCIEGE game has limited security functionality. This research proposes improvements to the current CyberCIEGE firewall functions. Some of the proposed refinements aim to reduce confusion when educating students about the basic concepts and functions of a firewall.

D. CHAPTER OVERVIEW

Chapter II gives an introduction to the evolution of networking, packet filtering and application gateways. This is to allow the reader to have sufficient background to understand the remaining information presented in this document.

Chapter III presents a description of the existing scenarios that relate to filtering components and some possible ideas that can be introduced to the existing scenarios to make the filtering topics more educational. A roadmap of what is expected to be achieved in the development of the scenarios is mentioned and a strategy is described for using CyberCIEGE elements to illustrate network filtering concepts.

Chapter IV provides a description of three scenarios on filtering. Users, assets, components, network topology, users' goals, conditions and trigger mechanisms that are implemented in each scenario are identified.

Chapter V reveals how the three scenarios were tested and the expected and actual results of those tests.

Chapter VI presents the conclusions and recommendations by the author based on this research and experimentation with CyberCIEGE.

E. SUMMARY

This chapter identifies the scope of this thesis and highlights to the reader the questions that this thesis attempts to answer. It also gives an idea of what to expect from the remaining chapters.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. CONTROLLING CONNECTIONS BETWEEN NETWORKS

In this chapter, the need for protecting networks from other networks is introduced, and different kinds of risks and attack types are discussed. Strategies for protecting internal networks from potentially hostile external networks are described. The firewall is introduced as an effective method of protecting internal networks from some kinds of threats.

1. Evolution of Computer Networks in an Organization

Decades ago, computer systems were stand-alone single user and multi-user systems. When personal computers further developed and the prices of computer resources started to decline, many organizations began to wire up their computer resources so that they could share computing services such as information, e-mail, and printing. This internal network, which stays within the boundaries of an organization, is usually identified as an intranet.

Computer networking started way back in the 1960s when time-sharing services were introduced to the public. In the 1970s, the Ethernet standard was developed, which allowed several computers to be connected to the same cable. A process of communication between computers on the same cable is described as follows. A computer can transmit information whenever the cable is not in use. In the event that two computers start transmission at the same time, a collision occurs. Both senders then wait a random amount of time before transmitting again. In any situation, every host/computer on the cable can receive every packet, and the hosts are expected to discard the packets that are not addressed to them. This scheme is known as Carrier Sense, Multiple Access / Collision Detect (CSMA/CD).

A host on an Ethernet can share resources with another host through the use of various network options. Some examples are:

- Peer-to-Peer networks

  This option allows two or more hosts to share files and access to devices such as printers without having to acquire a separate server computer. This

is mainly used for sharing content files/file sharing. The information stored across peer-to-peer networks is uniquely decentralized. Since a peer-to-peer host may have its own storage media that are accessible by other hosts, each host acts as both a client (information requestor) and server (information provider). A peer–to-peer network can be built with a coax bus backbone or 10BaseT cabling and a hub. It can be configured to allow the files or resources to be shared with anyone using another computer in the group. [2]

- File Transfer Protocol (FTP) program

  An FTP program allows files to be retrieved from and sent to another host. Most FTP programs have built-in features that allow users to control the flow of FTP data as either unidirectional or bidirectional.

- Servers

  Many servers have access control capabilities that allow user accounts to be created. In this way, servers can be configured to allow authorized users to have privileges to access information.

- Personal Computer Network File System (PC-NFS)

  NFS is usually installed to support file storage on a remote storage system so that it can be made to appear as a local drive on the host system. Information is sent through the network. NFS is useful on an internal network because it can be used to reduce the management burden.

With these enablers in network infrastructures, organizations are finding that an intranet provides a means for people to easily retrieve the information they need whenever they need it. However, these enablers may not be secure, because the information sent in the network may not be encrypted.

2. Connecting Intranets to the Internet

The Internet has evolved a great deal since its beginning. Its importance and influence have made a big impact on many people’s lives. Many organizations and

companies now regard the Internet as an essential channel to bring in business and to elevate their reputations to a higher level.

The Internet improves the data communication infrastructure for customers, suppliers, employees, and business partners. Information can be exchanged through uploading, downloading, and sharing of document files. Employees use the Internet as a tool to do research and gather information. E-mail and messaging allow them to stay in touch with customers, business associates, and coworkers. The greatest advantage of the Internet is the ease of access from anywhere in the world. In the past, road warriors had to ensure that they were equipped with the necessary data and documents before starting their journey. Today, road warriors can easily connect to the Internet to retrieve the information they need.

Some of the common Internet services available to organizations are:

- Telnet

  Telnet allows the user to run programs that are loaded on another computer. One must log in to a remote computer in order to manipulate files, run programs, read e-mail, etc.

- Electronic mail (e-mail)

  E-mail allows people to communicate through simple text messages. It is possible to send files as attachments with an e-mail message.

- World Wide Web (WWW)

  The WWW is accessed through a web browser, an application that runs on the user's computer. The use of the web is the fastest growing activity on the Internet. It can incorporate all Internet services.

Connecting to the Internet has become a common practice for most organizations because information is easily accessible as long as they are on the same network. The intranet can be accessed by the public by using the same tools and techniques, such as protocols and products that are used to access the Internet.

It has been highlighted by Alan McLaughlin that connecting the Internet to an intranet is a wonderful thing to do, but it also has a list of impressive threats.

> Intellectual property and trade secrets can be stolen and sold to competitors or customers, employee personal information can be accessed, or the network can be vandalized. [3]

Access control is usually used to protect an organization's sensitive data and systems. It restricts unknown or unauthorized users from access to information, hosts or networks. This protection mechanism is achieved by using authentication and authorization methods which associate a user with identification (ID) codes and passwords. Most operating systems and applications have this capability. Administrators can assign users rights and privileges to applications and data files based on user IDs. Operating systems can be configured to allow the grouping of users. This simplifies the administration of groups of users who require the same level of access to files and applications. Administrators are required to configure each and every host on the intranet. This can become non-manageable as a network grows with the organization.

B. FIREWALLS

A firewall is considered a useful access control mechanism and is defined as follows:

> A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. [4]

Generally, firewalls are used to prevent unauthorized Internet users from accessing private/organization's networks (Figure 1). All data entering or leaving the internal/trusted network passes through the firewall, which examines each packet and blocks those that do not meet the specified security criteria.

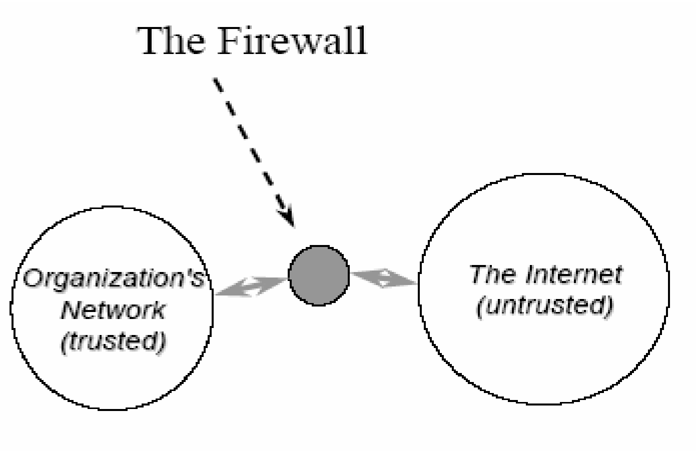


Figure 1 Firewall Illustration [From Ref. [5]]

A firewall can be used as a checkpoint as all traffic that needs to get in or out of a network has to be screened by this firewall. The administrators can focus the network security issues at this checkpoint, which is considered to be much more efficient than implementing security decisions and technologies onto every individual machine.

With the rapid growth of the Internet, there has been a noticeable increase in new vulnerabilities of Internet services. The administrator needs to be constantly aware of any new Internet threats and must update system protection mechanisms regularly. To maintain security, administrators must maintain all the systems by setting the correct access controls and by disabling vulnerable services in each machine. The possibility for errors is very high. Once a device on the network is compromised, it can cause a chain of disasters to the rest of the system. Thus, by forcing all traffic to pass through a single point of entry using a firewall, it is more efficient and effective for the administrator to catch bad traffic.

Firewalls can be deployed within a network to provide a means of containment that isolates one segment of the internal network from another, to prevent any compromise of security in one segment from spreading throughout the entire internal network.

Since the network protocol in the Internet is TCP/IP, and a firewall is usually deployed at a network boundary to provide filtering service; some attributes relating to TCP/IP must first be understood.

1. TCP/IP Networking

When systems on a network communicate, they need to speak a common language or protocol. One such protocol suite is Transmission Control Protocol (TCP)/Internet Protocol (IP). In Webopedia, TCP/IP is defined as follows:

> A set of communication protocols used to connect hosts on intranets and on the Internet. TCP/IP has become the de facto standard for transmitting data over networks. [6]

IP is the internetworking protocol. It is responsible for moving packets of data from one node to another. At each node, the IP header is used to forward each packet based on its destination address. Organizations connect to the Internet via an Internet service provider, which assigns the range of IP addresses to different organizations. The organization then assigns groups of their IP addresses to internal sub-networks within their intranet. IP headers are used to allow the data to move from sub-networks to organizational networks and subsequently to regional networks, and ultimately around the world.

TCP allows two hosts to establish a connection and exchange streams of data. A TCP header is used to verify the correct delivery of data from client to server. User Datagram Protocol (UDP) is an unreliable transport protocol that does not ensure the payload gets to its intended destination.

TCP/IP traffic is broken into packets. Figure 2 provides a simplified breakdown of a packet with the three key components: the IP header, the TCP or UDP header and the actual content of the packet.

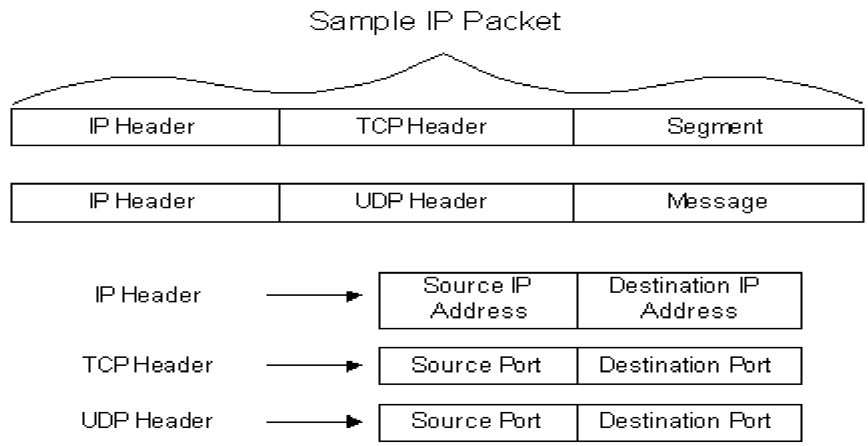


Figure 2 Simplified IP Header Model [From Ref. [7]]

a. IP Header

The IP header contains the IP addresses of the source, which is the sender, and the destination, which is the receiver. An IP address uniquely identifies a host.

According to Gerhard Cronje, IP is hierarchal to allow IP traffic to route which means that a single point of entry exists on most networks. One machine is able to control traffic to and from a network. [8] Detailed information of the IP can be found in RFC791.

b. TCP or UDP Header

Both TCP and UDP headers contain the source port of the sender and the destination port of the receiver to identify the applications that are sending and receiving the traffic. In addition, TCP headers contain additional information such as sequence numbers and the conversation state. The destination TCP or UDP ports define the location for delivery of the data on the server when the packet reaches its destination. More information of TCP and UDP can be found on RFC793 and RFC768 respectively.

c. TCP or UDP Port

The port number is used by a sender (client) or receiver (server) when sending or receiving messages. A port is identified by a 16-bit number which allows the port number to range from 0 to 65,535. Server processes are usually associated with a fixed port, for example, 25 for SMTP and 80 for HTTP. The port number is "well-known" because it needs to be used when initiating a connection to a particular host or service. On the other hand, the client operating system generates a random port number.

Port numbers are usually grouped based on the type of services. Both TCP and UDP use port numbers to keep track of the communication sessions. A list of TCP and UDP well-known port numbers can be found on http://www.iana.org/assignments/port-numbers.

2. Packet Filtering

The ability of a firewall to filter network traffic is based on the properties of the TCP/IP protocol. With simple packet filtering, the filtering mechanism uses a simple ordered list of rules. For example, when a packet is received in a firewall, it is scanned against all the rules, and the action (either permit or deny) is determined by the list of rules. If a packet does not match any of the rules, a default action is applied. Each network interface can have its own list of rules.

The rules can make use of the following fields from the IP protocol header: source address, destination address, TCP/UDP source port numbers and TCP/UDP destination port numbers. These define the filtering as follows:

- To block connections from specific hosts or networks.
- To block connections to specific hosts or networks.
- To block connections from specific ports.
- To block connections to specific ports.

The configuration of the filtering rules can be set up to specify any ports or hosts.

a. Inbound and Outbound

The terms "inbound" and "outbound" are usually used to refer to the direction packets are traveling, from the point of view of the protected network.

An "outbound connection" is a connection initiated from a client on an internal network to a server on an external network. The connection includes both outgoing packets from the internal client to the external server and incoming packets from the external server back to the internal client.

An "inbound connection" is a connection initiated from a client on an external network to a server on an internal network. The connection includes both incoming packets from the external server to the internal client and outgoing packets from the internal client back to the external server.

In practice, most people will focus on the inbound filtering more than the outbound filtering.

b. The Last Rule of Firewall Configuration

There are two access denial methodologies used by firewalls for the rule set. These two approaches have opposite effects, yet the intent for both is to control access. The two approaches that are mentioned in the MOREnet's technical support are:

- *Everything not specifically permitted is denied.*
- *Everything not specifically denied is permitted.*

Since a firewall only allows traffic that meets its set of rules to pass through, it is important to note that there should be a last rule, which is commonly overlooked. The mistake of overlooking the last rule can be disastrous as it may undermine the functionality and security of the network.

(1) Everything Not Specifically Permitted is Denied

This is a proactive approach which works on the premise that all access is denied until a filter rule is configured to specifically allow access. Effectively, it is considered to be secure by default but it can be regarded as too restrictive. In many instances, legitimate traffic suffers until the correct settings are identified and implemented to allow that traffic to pass. [9]

(2) Everything Not Specifically Denied is Permitted.

This takes a reactive approach which works on the premise that all access is allowed until a filter rule is configured to specifically deny it. Although it is considered to be a less secure approach, it is more flexible because legitimate traffic is unlikely to suffer. [9]

c. Types of Packet Filtering Firewalls

Conceptually, there are two types of firewalls packet filtering and application gateway firewalls. Regardless of the type of firewall deployed, all the firewalls provide the same basic feature: to control inbound and outbound traffic.

(1) Packet Filtering Techniques. A packet filtering firewall normally screens packets at the IP network layer. The filtering decision is made based on information in the IP packet header. The information contained in the IP header is

compared to a pre-configured set of rules. A deny or permit decision is made based on the results of the comparison. The filtering process depends on some or all of the following fields:

- Source IP address: the address the data is coming from.
  The source address can be used to allow only traffic from a specified IP address to access the network. This is useful if a remote site must access the network. This field can be used for opposite effect. For example, it can be used to deny access to a known malicious network or competitor. [10]

- Destination IP address: the address the data is going to.
  The destination address field can be used to restrict access to resources on a public network that should remain private. An example would be a server on a corporate network that contains sensitive data such as employee personnel information. Public access to this sensitive storage system can be denied through filtering the destination IP address.

- Source and destination port: the session and application ports being used to transfer the data.
  Different forms of communication over a network use specific ports. For example, HTTP or web service request uses port 80. Filtering out all packets not destined for port 80 will prevent unauthorized access to that web server. Alternatively, if a web server is sending packets via any other port than port 80, the packets can be filtered. [7] A client will generate a source port number that is above 1023 (assume 1024 in this case) to establish a connection to a server. The client connects to the server based on a well-known port such as 80 for the web server (HTTP). When the server returns a reply, it sends information that departs from that well-known port 80 and arrives at the client port 1024 that was initially selected. Thus, a packet filter can determine which services are to be filtered, depending on the port information.

- Protocol type (TCP/UDP):
  The protocol field identifies what types of packets are being used in the transmission. Using the prototype field, the filter can restrict the type of packet entering its protected network. For example, UDP packets are usually used for video streaming, which can be dropped before entering an enterprise network. This might be done to prevent employees from downloading movies which could consume a lot of computing resources.

- Session state:

> Some filtering devices are state conscious, which allows the device to remember the session state information throughout the connection. For example, incoming TCP packets are allowed to enter a network only if they are responses to the permitted outgoing TCP packets.

Packet filtering can take on two forms: static filtering and dynamic filtering.

(2) Static Packet Filter. Alan McLaughlin states that a static packet filter is a prioritized list of rules and all rules are created by an authorized administrator and stored in a database. These rules do not change without the direct intervention from the administrator. A packet may match more than one rule but the rule appearing first on the list shall take precedence. The static packet filter does not use the state field to make the decision. [3]

(3) Dynamic Packet Filter. This is also known as stateful packet filtering. Dynamic packet filtering evolved from the need to accommodate certain features of the TCP/IP protocol suite. The idea behind dynamic packet filtering is to introduce the concept of state awareness. A rule is dynamically created when a session is initiated from the protected side of the filtering device's interface. It will remember that session by noting the source and destination IP addresses, source and destination ports, and the protocol of the request. From this point on, any response packet attempting to enter the protected network is required to have an exact match with a session stored in the dynamic state table for inbound filtering. This rule remains in the dynamic state table until the session has been terminated. This helps to prevent any unsolicited packets from entering the network. On the other hand, if a connection request is received from outside the protected network, the packet is subjected to the pre-configured set of rules.

(4) Comparison between Static and Dynamic Packet Filtering. According to Microsoft, dynamic packet filtering shares the strengths and weaknesses of static packet filtering firewalls. The main difference is that static packet filtering does not keep track of the state of network packets, such as whether it is the first, middle, or last packet. It does not know if the traffic is associated with a response to a request or is the start of a request. On the other hand, dynamic packet filtering keeps track of the state of the connections, which gives dynamic packet filtering the capability to tell if the traffic is

associated with a response or request. With the implementation of state consciousness, dynamic packet filtering firewalls are generally considered to be more secure than static packet filtering firewalls. [7]

Some researchers claim that dynamic packet filtering can accommodate other network protocols in the same manner as static packet filtering, but in actuality dynamic packet filter technology is applicable only within TCP/IP network infrastructures. [11]

(5) Comparison between Hardware and Software Firewalls. All firewalls have firewall software programs running on a hardware platform. Both hardware and software firewalls are designed to achieve the same goal and that is to filter off unwanted traffic. The terminologies of hardware or software firewalls are used by most marketers to distinguish their products.

A hardware firewall has a firewall program running on a dedicated platform. The filtering process is regarded to be faster and more reliable than a software firewall. Software firewalls, unlike hardware firewalls, are usually installed on individual computers such as a server and run automatically in the background, which may impact their performance.

3. Deploying Firewalls

This section describes the deployment of a firewall. Many organizations have the objective of deploying a firewall to increase their information security level in terms of confidentiality, integrity, and availability.

a. Host Based Firewall

A host based firewall is software that installs on a computer to restrict the type of traffic that is allowed in or out of the computer based on specific applications. They are also known as personal firewalls and are often added on to workstations and/or servers. Usually, host-based firewalls are an effective mechanism because they are only responsible for a single host’s protection.

b. DSL Routers and Other Equipment

The rise of awareness in information assurance has led to the demand for the integration of a firewall mechanism in network equipment such as cable modems, DSL routers, and wireless base stations. As highlighted in Section 2, many Internet

services are readily available, but whether the services are those of friends or foes all depends on how they are being used.

For example, NFS can be used on an internal network to allow sharing of resources. However, NFS can be exploited by outsiders to access the internal network information. With a firewall incorporated on a modem or router, it can help to reduce the risk of exploitation of the Internet services up front of the Internet connection.

c. Dedicated Firewall

A dedicated firewall usually sits between two networks, a private network and a public network such as the Internet, to handle the heavy traffic load. This type of packet filtering firewall is efficient in blocking certain types of potential threats by filtering unwanted protocols. A dedicated firewall is also known as a boundary firewall.

d. Internal Firewall

In most modern applications, firewalls and firewall environments are usually associated with the context of Internet connectivity and the TCP/IP protocol suite. However, firewalls can also be deployed in network environments that do not require Internet connectivity. Therefore, a firewall can be defined as a system or a group of systems that enforce an access control policy between two networks or protect a trusted network from an untrusted network. It can be used internally to prevent unauthorized access to a particular subnet, workgroup or LAN within an organization's network. For example, many corporate networks employ firewalls to restrict connectivity within internal networks. They might prevent access between the Engineering department and the Accounting department. By employing firewalls to control connectivity to these areas, an organization can prevent its internal personnel from accessing sensitive systems and resources.

The effectiveness of a firewall solution depends on two factors:

- The firewall solution, either a stand-alone system or software-based running on a dedicated system, must be physically located in a safe place. If the system is compromised, the firewall will not be effective.

- All traffic to and from a trusted network must pass through the firewall. If a firewall can be bypassed, there is no assurance that the network is safe.

4. Limitation of Firewalls

It is important to understand that a firewall, regardless of how sophisticated or technologically advanced it is, will not be able to make a computer immune to attacks. To achieve greater protection, a firewall should be used with other security measures, yet there is still no guarantee that the network will be 100% secured. In short, there is no perfect solution. Firewalls are usually deployed as a complement to a layered defense. Firewalls create obstacles to discourage or delay attacks. Thus, firewalls can be very effective in blocking most attackers from compromising an individual computer, but it is difficult to prevent every possibility of intrusion.

a. Internal Threats

A firewall often cannot offer protection against insider attacks. Since the users are already on the internal or trusted network, they often have access to the protected services without having to go through the firewall. A firewall cannot stop malicious insiders from attacking other systems inside the firewall, but it can help to prevent attacks from the inside network to the outside one.

b. Unable to Detect Tunneling Through a Firewall

> A firewall cannot always prevent tunneling where one kind of protocol is wrapped up inside another. [12]

Malicious traffic can be disguised as legitimate traffic, which the simple packet filtering cannot handle. The malicious traffic can tunnel through the allowed ports on the filter.

c. Unable to Distinguish Data Sensitivity

A firewall is unable to distinguish the sensitivity of the data encapsulated inside a packet. As a result, information can leak out via a legitimate packet.

d. Exploitation of Security Holes

A firewall has limitations in understanding the full context of the TCP/IP protocol suite. As a result, exploitation of the TCP/IP is still increasing. For example, assume a firewall is set to deny e-mail programs from receiving and/or sending messages,

yet allows a web browser to browse the Internet. It is possible to use the web browser to retrieve and send e-mail, thus bypassing the intent of the firewall rules.

5. Application Gateways

An application gateway is considered to be one of the better and improved firewalls. The packet screening can be complex and it is implemented for a system configured with at least two network interfaces. MOREnet technical support states:

> The application gateway acts as an intermediary between two endpoints: one from the source to the gateway and one from the gateway to the destination. Each endpoint can only communicate with the other by going through the gateway. When a client initiates a request from the untrusted network, a connection is established with the application gateway. The gateway determines if the request is valid by comparing it to a set of rules and then sends a new request on behalf of the client to the destination. [9]

This approach avoids a direct TCP connection between a trusted network and an un-trusted network. It is important to note that the application gateway actually builds a new request, only copying known acceptable commands before sending it on to the destination, which is known as full packet awareness. [13]

a. Advantages of an Application Gateway

Application gateway firewalls have many advantages over static and dynamic packet filtering firewalls. Application gateway firewalls usually have extensive logging capabilities due to the firewall being able to examine the entire network packet rather than just the network addresses and ports. Another advantage is that application gateway firewalls allow administrators to enforce the type of user authentication that is appropriate for a given organization network infrastructure. Application gateways are capable of authenticating users directly, whereas the packet filtering firewalls normally authenticate users based on the network layer address of the host. As network layer addresses can be easily spoofed, the authentication capabilities in an application gateway are much superior to those of the packet filtering firewall. [13]

b. Disadvantages of Application Gateway Firewalls

The advanced functionality of application gateway firewalls also results in several disadvantages as compared to packet filter firewalls. According to NIST, the “full packet awareness” in application gateway firewalls requires more resources such as time,

memory, and power to process each packet. Another disadvantage is that application gateway firewalls have limited support for new applications and protocols. [13]

C. SUMMARY

This chapter gives an introduction to the evolution of networking, packet filtering and application gateways. This is to allow the reader to have sufficient background to understand the remaining information presented in this document. An important point to note is that the difference between dynamic and static filtering is the "connection state" which allows the dynamic filter to understand the direction and the sequence of the packets.

In the next chapter, how CyberCIEGE can be used as an educational platform for demonstrating filtering shall be discussed.

III. USING CYBERCIEGE TO ILLUSTRATE NETWORK FILTERS

A. EXISTING SCENARIOS

Currently, CyberCIEGE has a set of scenarios available on-line at http://cisr.nps.navy.mil/CyberCIEGE/scenarios.html. In general, each scenario has a three-dimensional (3D) environmental view which represents an office or military-based floor plan, users, and assets which the game developer initiated. The scenario consists of several phases and objectives to illustrate specific security issues which are valuable and informative for players. Each player has to satisfy all the objectives in each phase to beat the scenario which means the player must ensure that the organization in the game is making money; i.e. the users are achieving their goals, and there is no violation of the organization security policy. [14]

During the initial phase of this thesis research, the two games named *Introduction Scenario* and *TirePly Filters Scenario* were explored. These two scenarios are examples of how CyberCIEGE represents network filters. Below is the brief description of each scenario and its educational value related to filters or firewalls.

1. Introduction Scenario

This scenario guides the players to understand the mechanics of the game and introduces the player to a number of the CyberCIEGE security concepts. [15] The objective of the firewall/router concept in this scenario is to set up the filter rules to allow only some application services to access the Internet. The objective did not clearly specify which application services should be allowed or denied. This may cause confusion to an entry-level player. The scenario for the filter portion of the introductory scenario closely resembles one of the objectives of the *TirePly Filters Scenario*. The filter aspect of this scenario does not add any value beyond that provided by the *TirePly Filters Scenario*. Thus, if the filter portion was removed, the scenario would be improved.

2. TirePly Filters Scenario

This scenario explores the issues arising from connecting networks to the Internet and the use of filters to protect assets. [15] It also illustrates a good concept: that filtering devices is not a perfect solution even though the filtering rules are properly set. Physical

isolation of a network system from the Internet may be a better way to protect a high value asset.

3. Findings

a. Takeaway Lessons

By playing the two interactive scenarios discussed above, a list of key ideas related to firewall or filtering components was noted.

(1) Internet Vulnerability. As described in Chapter II, both the scenarios illustrate that the Internet is essential to organizations to carry out their tasks. However, direct connection to the Internet may not be ideal as it will expose the organization's asset to the world. This is unacceptable in the scenarios.

(2) Firewall as Access Control. Using a properly configured filtering component increases the level of confidence in assuring protection of information in the systems. The filtering component can be used to deny vulnerable protocols such as telnet service applications.

(3) Player Interface to Filter. The player need not be concerned about the details of the IP source and destination addresses, the type of protocol (UDP or TCP), or the TCP/UDP port number. The filtering setup interface in CyberCIEGE is meant for a player to be aware of some of the application services that are commonly used in an organization. A player can choose to deny or permit the filtering rules based on the scenario requirement. The interface helps to illustrate to the player that filtering can be done on either inbound/outbound network traffic, or both.

(4) Isolation, the Best but Overlooked Solution. Although a firewall is one of the key elements for strategic defense of digital information on a network, it is often forgotten by many professional IT administrators that isolation could be the best solution. In the scenario, many players including this author, bought the most expensive and sophisticated devices in an attempt to secure the high value assets. However, the assets were still being accessed by attacked. The lesson learned is that stand-alone systems without connections to networks have fewer opportunities for externally based attacks, and therefore maybe the best option.

b. Adding New Educational Value

To improve the educational value in regards to the filtering components, more filtering-based scenarios need to be available. These identified issues are used as objectives to build the add-on scenarios for this thesis research.

(1) Novice Issue. The graphics of the games are very attractive, but there are some difficulties in understanding some of the content in each tab field in the scenarios. Although there are movie clips that help players to understand the features in the game, familiarity with the functions and contents in the game is achieved only after many rounds have been played. This can be further improved by introducing a step-by-step hands-on guide and explanation for novice players. The needs of a novice player of the game were taken into consideration for the research in the firewall scenarios.

(2) Missing Element in Filtering Components. Generally, the existing scenarios that deal with the filtering component do not clearly introduce the behavior of the filter device. There is no clear indication of the type of filtering mechanism, how the rules are applied, or how it will respond. In order to demonstrate the "missing" element for an inexperienced CyberCIEGE player, a sequential build-up approach was adopted to guide and re-enforce the player's knowledge of the filters.

(3) Internal IP Spoofing. One of the potential vulnerabilities that an organization can face is IP spoofing. A filtering device such as a firewall, regardless of the type of filtering mechanism, can be an effective tool to minimize some IP spoofing attacks. For example, if the firewall is deployed between an internal (trusted) network and Internet (untrusted) network, the filtering rules on each side of the firewall interface can be set up to identify internal IP spoofing. The firewall can be configured to drop all incoming traffic that uses any address of the internal network as a source IP address. Similarly, a firewall can deny someone from on the internal network from spoofing an external IP address. However technologically inclined administrators may overlook this issue because they may handle a long list of rules. Therefore, this important scenario should be implemented to create awareness of IP spoofing.

(4) Firewalls can be used for Internal Network. A firewall is commonly used at the checkpoint between the Internet and internal network which is clearly illustrated in the scenarios. However, a firewall can also be deployed within an

organization to restrict employees of one section from accessing resources in another section. This scenario, which was missing, should be included to highlight this additional function of a firewall for securing an internal network.

(5) Application Services. There are many application services on the Internet, and more to be introduced. It might be inefficient for a system administrator to have to constantly adjust the firewall rules to deny the latest insecure application. Therefore, it is wise that the players should take a proactive approach. This means that the player should block all application service requests in an organization and only permit specific service requests to pass the filtering device, upon approval by management.

(6) Introduce Demilitarized Zone (DMZ). The existing scenarios that involve the use of filter devices have illustrated some of the possible issues that an organization would encounter. With a clear understanding of how the firewall functions, further research on the deployment of the firewall in terms of the organization's network topology should be introduced. A demilitarized zone (DMZ) was selected, as many organizations in the industry have implemented the concept in their environments. The existing firewall/router component in CyberCIEGE shall be used to model a DMZ environment, evaluate whether the scenario is feasible, and conduct an experiment to determine the educational objectives related to the security issues that could be brought across to a player.

B. CYBERCIEGE GOALS

The goal for the development of these new scenarios is to complement the existing scenarios to give the potential players, i.e., students in an introductory computer security course, further experience in managing major issues, strategies, and tools involved in network security and to see if they can synthesize what they have learned about firewalls from course materials.

1. Player Goals

- To increase the player’s awareness of the security issues, deployment strategies, and tools for computer and network systems.
- To allow the player to experience an attack in order to better understand the strategies, strengths and weaknesses of defense mechanisms, and

mindset of the attackers, as well as to be able to react defensively in a "simulated" environment.

- To give the player a foundation for the application of the knowledge he/she acquires in the scenarios and contribute his/her skills in future work as an information assurance professional.

2. Game Developer Goals

- To use the CyberCIEGE tools to build a "simulated" real world environment for defenses and attacks that will contribute to the player's learning.

- To improve and expand CyberCIEGE's potential value as an educational teaching tool.

C. INFORMATION ASSURANCE

In the CyberCIEGE world, the destiny of an organization's information security lies in the hands of the players. The player will have to decide on the best option to balance among the security of information, functionality of the organization, and limited resources. In each scenario, an environment is created that is comprised of a set of predetermined users and assets. An asset, which represents information that can have low to high sensitivity, is assigned to users or belongs to the organization. The assets reside in a workstation or server on an organization's internal network. Access to an asset can be assigned to more than one user.

The assets have associated motive values that determine the strength of attack against the assets. Different motive values will attract different types of attacks such as Trojan horses, viruses, unskilled hackers, professional hackers, and others. The attacks also include bribery of the users in the internal organization that could compromise the assets through physical or remote access. These random attacks are statistically generated by the CyberCIEGE attack engines that will constantly search for and launch an attack on high motive assets, which may cause the player's failure in achieving his or her goals.

Finally, the player has the option to purchase new defense mechanisms or use existing defense mechanisms to deploy his or her strategy to protect the assets from attacks. The player not only needs to know how to strategically place his or her defense

mechanism, such as a firewall, he or she also needs to set up the filtering rules to ensure only intended traffic is permitted. If the filtering rules were not properly setup and results in the failure to satisfy all the users' needs to access the required assets, or the failure to protect the assets from unauthorized access, the player will lose the game.

In the game, the measurement of a player's ability can be determined by the amount of money available to the player. For each successful completion of a phase or objective, the player gets to increase his/her money. However, any compromise of an asset, or any delay in achieving the goals may lead to a decrease of his/her amount of money. For example, in all three scenarios the initial amount is a baseline. When the game starts, every simulated hour, a decrease in the money is activated when a goal is not met. Different goals will cause different amounts of money to decrease. When an objective is met, a lump sum of money is rewarded.

D. CYBERCIEGE TOOLS

In CyberCIEGE, the scenarios are developed using a Scenario Development Tool (SDT). A detailed description of the usage of the SDT can be found in the CyberCIEGE Scenario Development Tool User's Guide. This section shall provide an overview of how the CyberCIEGE elements can be used to construct and demonstrate the scenario in terms of filtering.

1. Assets and Attack Engine

CyberCIEGE "assets" are used to represent information resources. Different assets can have different values to the enterprise and attackers. The values of the assets are based on the negative impact that their unauthorized disclosure modification or lack of availability would have on the organization. Assets with a moderate secrecy motive can be used to attract game engine attacks. This is done by setting each asset with a non-zero value on the attacker motive field.

In the three scenarios developed for this thesis, the game engine attack was not used. The main focus of the scenarios was to provide continuous feedback to the players, to let them know whether or not they have successfully achieved the users' goals, and whether or not they have created insecure configurations. Since all three scenarios provide feedback to players before attacks would occur, the attack engine is not needed.

Assets are used in these scenarios primarily within user goals, described below in the Users and Goals section.

2. Components

A list of components is available in CyberCIEGE. Several components such as a workstation, servers, and firewalls/routers are used in the scenarios. An asset or several assets can be assigned to reside in a workstation or server. The firewalls or routers provide a means for connecting two or more different networks together, and are used to block or permit different types of application services between networks.

3. Networks

CyberCIEGE "networks" are used to represent a communication medium that provides a means for components to be interconnected. It allows the components to be connected in a local area network (LAN). The number of LANs in each scenario can be specified by the game developer. Each LAN can be configured as static or non-static. When a LAN is static, the player cannot change the topology of the network.

In this thesis, three types of networks are considered.

a. Closed Network

An internal closed network is considered to be a trusted network that allows its employees to communicate and share resources within an organization. It can be made up of one or more LANs. The traffic does not go beyond to the Internet. Closed networks provide a good simulated environment to understand about filtering. In Scenario 1 of this thesis, two LANs were connected to a firewall/router to form the simplest closed network as shown in Figure 3. The two LANs were configured as a static network because the objective is to assess whether the player is able to setup the filtering rules. Changes to the topology of the network were the least concern. However, Scenarios 2 and 3 require the player to change the topology network.

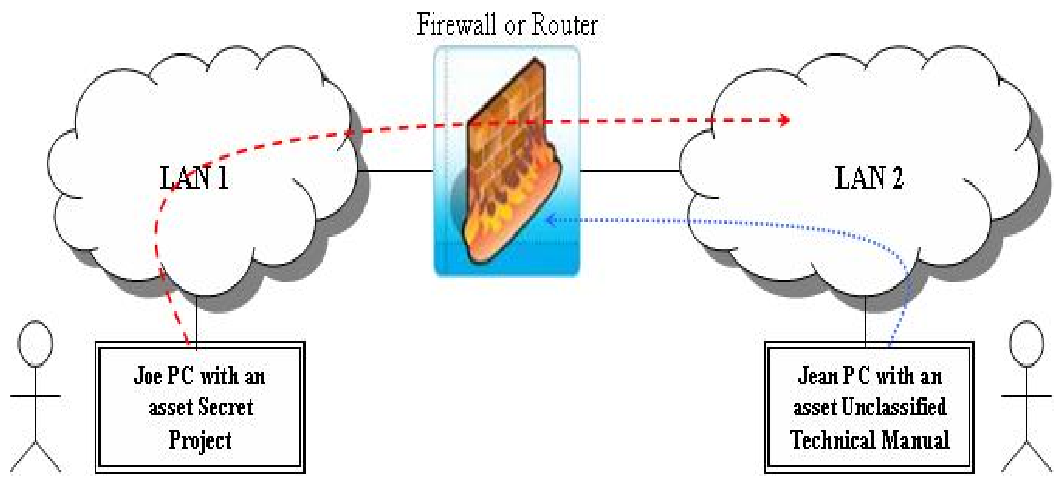


Figure 3 Simple Scenario 1

b. Internet

In CyberCIEGE, "Internet" is an external network that is already predefined in the SDT. This element does not need any definition setting. The game developer has the option to decide whether the Internet connectivity is available in the scenario. In Scenario 1, the Internet option was made unavailable, as the game does not require any Internet connectivity, whereas Scenario 2 and Scenario 3 involve the Internet connection to introduce more challenging security issues for the player.

The Internet can be used to provide a logical connection for two or more physically separated networks as shown in Figure 4. In this way, the network in the headquarters office and the network in the production plant are connected through the Internet. In Scenario 2, an employee without any authority to access information in the headquarters office is located at remote Internal Network 3. If this employee were malicious, he or she might spoof an internal IP address of network 1 and/or network 2.

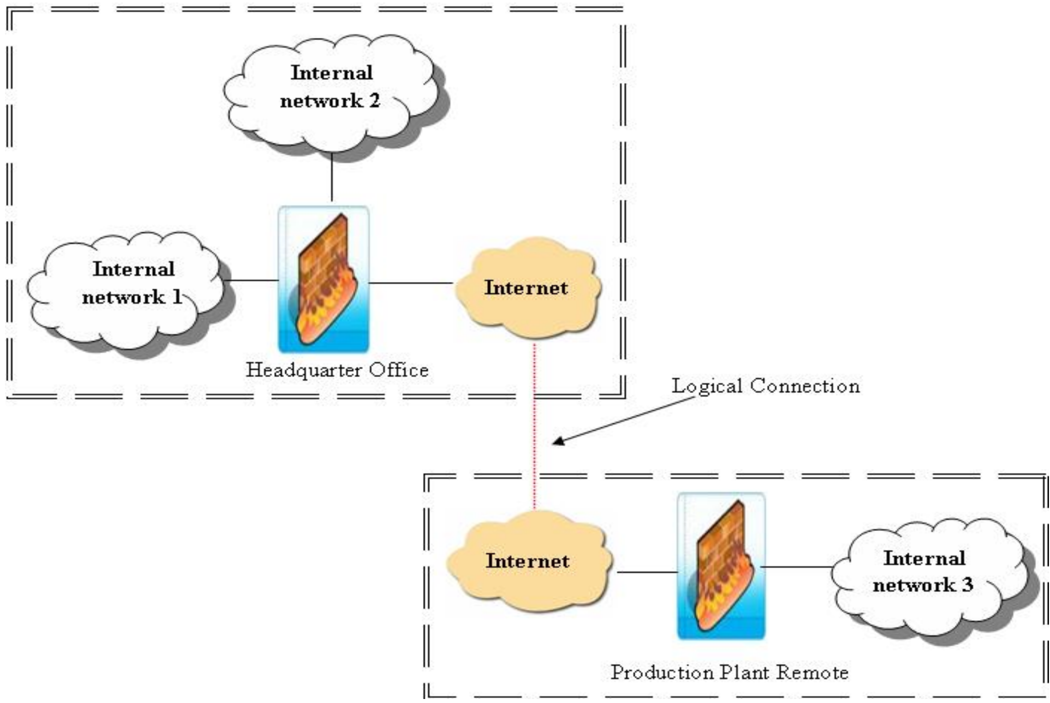


Figure 4 Network Connectivity via the Internet

c. Demilitarized Zone, DMZ

A DMZ is a network that is usually deployed between two firewalls. It is considered to be neither an internal network nor the Internet, and is often managed by the administrator from the internal network. Any information or resources that can be accessed by the public are usually deployed in this network, thus protecting the internal network from public access.

In CyberCIEGE, a "physical" DMZ can be created by deploying the network components (workstations and servers) in-between two firewalls, as can be seen in Figure 5. The effectiveness of a DMZ depends on the rules on the two firewalls set by the player. In Scenario 3, two firewalls, two workstations, two private servers, and an internal network were made static. This is to ensure that the player will deploy a DMZ as a solution. The player needs to use the DMZ topology and set the filtering rules on both firewalls to manage the access control on the assets on all the servers.

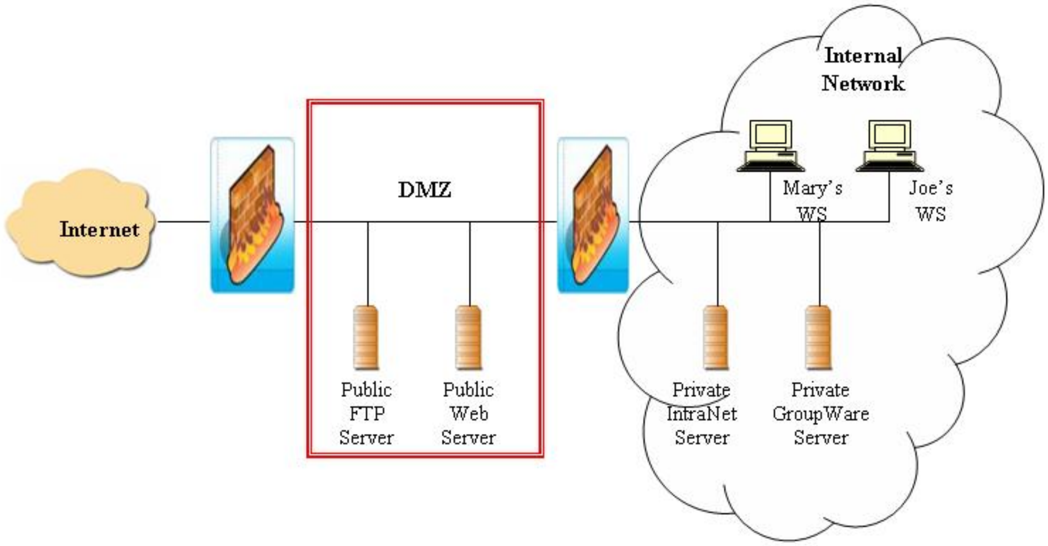


Figure 5 Internal Network with a DMZ

4. Users and Goals

In CyberCIEGE, "users" and "user goals" are typically used to generate revenue for the enterprise. The productivity and happiness of users depends on the status of users' goals. When the user goals are met, the users' happiness and productivity remains high.

In each scenario, each user is assigned single or multiple goals. A user goal is to access an asset over a network using specific application services. With a firewall in-between the networks, the player has to make the correct choice to allow the appropriate application services to pass the firewall. This then increases the happiness of the users.

For example, in Figure 3, a workstation on Network LAN 1, is assigned to Joe and another workstation on Network LAN 2, is assigned to Jean. The assets, Project Firebird and Technical Manual, are instantiated on Joe's workstation as well as Jean's workstation upon the start of the game. Joe is assigned a user goal to access the Technical Manual with the Database application service. At the LAN 1 firewall's interface, the filter rules were initially setup to deny all application services and only allow the Database application service to LAN 1. At the LAN 2 firewall's interface, all application services are allowed. This implies that Jean is able to reach the asset Project Firebird and Joe is unable to access the asset Technical Manual. Thus, Joe is unable to fulfill the user goal, which will cause a trigger mechanism (CashTrigger) to penalize the organization's revenue. The CyberCIEGE game engine will reduce the value of Joe's productivity and

happiness. When the player successfully configures the filter rules such that Joe is able to achieve the user goal, Joe's productivity and happiness will increase.

5 Objectives and Phases

Each scenario can be divided into several phases and the player needs to fulfill one or more objectives in each phase. The objectives and phases mechanism in CyberCIEGE allow the difficulty levels of the scenario to be built up gradually. Each phase allows the player to focus more on specific security issues of the filter. In Scenario 1, there is only one phase with one objective. For Scenarios 2 and 3, the level of difficulty increases and the player has to complete three objectives in three phases. The purpose of the phases and objectives is to walk the players through the game such that they know when to change the network topology.

6. Conditions and Triggers

The scenario developer establishes a set of conditions that can be used by the game engine during run-time to activate some actions. A single condition or a set of conditions can be used to determine the outcome of an action. For example, if a player fails to configure the filter device properly, then the public from the Internet is able to access the high motive asset. This can be measured by using a set of conditions that can be used to trigger some action. There is a list of trigger mechanisms available in the SDT, which have their own unique application.

Conditions and triggers are primarily used in all three scenarios to assess the application services in connection to an asset, as explained below.

a. Conditions

The connectivity between asset and network is assessed by two condition classes, "AssetToNetworkByFilterType" and "AssetToNetworkFilterCount". The "AssetToNetworkByFilterType" condition allows the game engine to determine whether an asset can be accessed from a predetermined network using a particular application service. Both conditions are used to measure the network connectivity to an interested asset.

For example, in Figure 6, the AssetToNetworkByFilterType is used to measure the access connectivity from the Internet to assets residing on Network 2. This means that the asset, employee personnel data, on Internal Network 2 can be denied by

both or either of the firewalls. The number of firewalls between two end networks has no effect on the result of the AssetToNetoworkByFilterType condition. If there are ten firewalls and only one of them is used to deny an application service, the output of AssetToNetworkByFilterType would show a positive result. In the three scenarios, this condition is used to determine whether the player has allowed a specific application service to reach an asset.

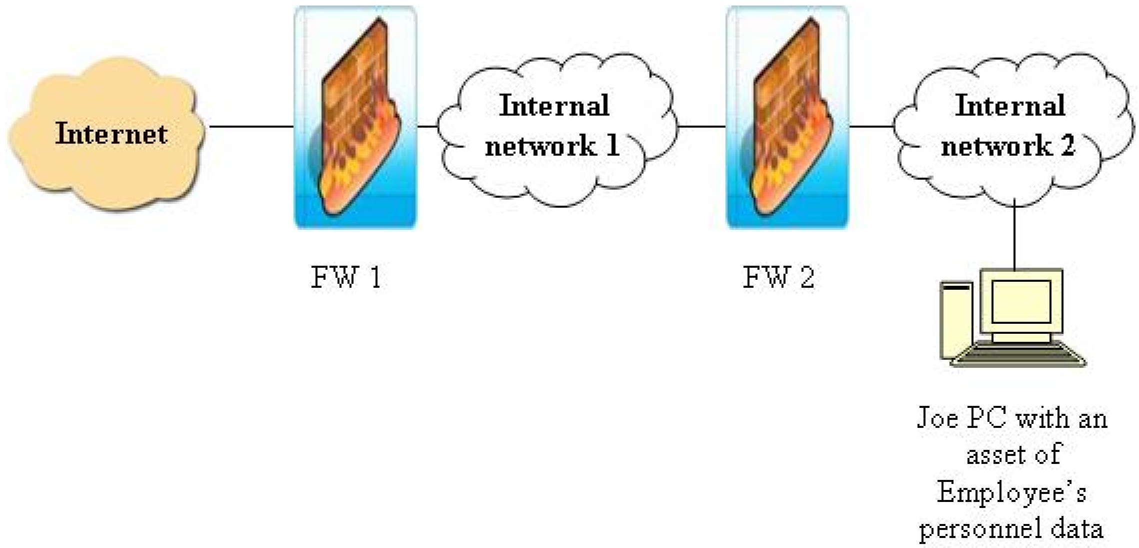


Figure 6 AssetToNetworkByFilterType Illustration

"AssetToNetworkFilterCount" is a new condition class introduced to the game developer. This condition allows the game engine to measure the number of application services that can be used to access an asset from a specified network. This condition counts the number of application services that have network connectivity from one end of the network to the other end of the network that has the asset. In all three scenarios, this condition is used to assess whether the player has blocked a minimum sum of services.

By combining the two conditions, it would give a good assessment on whether the player has configured the rule correctly.

b. Triggers

The trigger mechanisms provide a means for interacting with the player. Triggers can be set to go off based on a combination of conditions. The trigger class that is often used in a scenario is "TickerTrigger" and "SpeakerTrigger". They are used as

visual warnings and hints before an attack occurs. The TickerTrigger is used to display a message at the bottom of the screen while the game is still on run-time, while SpeakerTrigger displays a message cloud over the user's head. The trigger mechanisms are activated only when a set of conditions are met. In the three scenarios, TickerTrigger is configured to activate messages periodically, about every two hours in terms of scenario time. It provides negative feedback to the player that an error was made on the filtering rules. SpeakerTrigger is used to highlight to the player that the users are not happy because they could not achieve their user goals.

E. SCENARIOS ROADMAP

The strategy for building the game has been discussed in Section D. There were some initial doubts about the filtering mechanism which needed further investigation before scenario development could begin. The initial questions were:

a) What type of filtering mechanism does the CyberCIEGE filter model use?

b) How may the representation of IN and OUT be improved for the filter component?

c) Does the sequence of filtering rules have any impact on the filtering process?

The investigation provided an adequate understanding of the CyberCIEGE filter mechanism. The three scenarios were then proposed as follows:

a) A scenario for a novice player to understand filter principles in CyberCIEGE.

b) A scenario to illustrate the potential threat of IP spoofing.

c) A scenario to illustrate the use of a DMZ.

F. INVESTIGATION OF PACKET FILTERING

This section describes the process of an experiment that was carried out to determine the characteristics of the filtering mechanism in CyberCIEGE. A weak conclusion was established from the results collected from the experiment and a suggestion was made to improve the game.

1. CYBERCIEGE Filter Component

The behavior of the filtering mechanism in firewall or router components was carried out. The existing *TirePly Filter Scenario* was used as the platform to determine what kind of packet filtering is represented in CyberCIEGE.

The phase 1 objective of the pre-existing *TirePly Filter Scenario* is to connect Larry's computer to the Internet so that Larry can access a Web Server on the Internet. First, the network topology was re-wired such that a filtering device (firewall or router) was connected to Larry's computer and the Internet via the network internal LAN 1 and the Internet, respectively, as shown in the Figure 7. By default, the filtering rules on the application services were not blocked as shown in Figure 8. This implies that Larry's goal is achieved as the web services request was allowed to the Internet, which can be verified on the USER Tab as shown in Figure 9. It should display "Asset Failure: None".

Thus, by varying the different combination of inputs on the TO and FROM on the filter, the output of the filter can be observed on the USER Tab, user's goal. The results were tabulated and are shown in Table 1 and Table 2.

Figure 7 Connect Larry's Computer to Internet

Figure 8 Default Services Not Blocked on Firewall

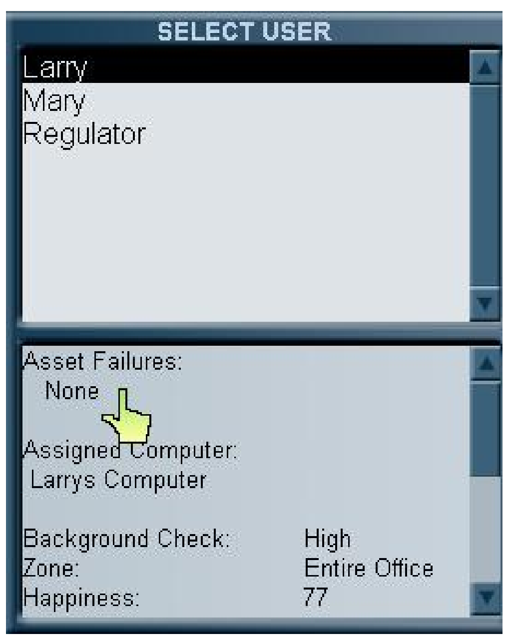


Figure 9 Larry’s Goal

Application Service	To	From	Asset Failure
Web Server	[ ]	[ ]	None
Web Server	[X]	[X]	Web
Web Server	[X]	[ ]	Web
Web Server	[ ]	[X]	None

Table 1 Truth Table of Web Server Service on Internet Interface of Filter Device

Application Service	To	From	Asset Failure
Web Server	[ ]	[ ]	None
Web Server	[X]	[X]	Web
Web Server	[X]	[ ]	None
Web Server	[ ]	[X]	Web

Table 2 Truth Table of Web Server Service on Internal LAN1 Interface of Filter Device

2. Filtering Interface to the Player

The graphical user interface for the filtering rules of the filter component has an "IN" and "OUT" label which represents the inbound and outbound interface of the firewall. The labels can be misleading, especially for people who are exposed to filtering for the first time.

For example, an employee in an internal network needs to access web browsing. Therefore, the internal network cannot be completely sealed off from the Internet. On the other hand, the internal network should not be accessible by the public in the Internet via this opening. If the inbound traffic (IN) is blocked, does that mean the response from the web server is blocked? Likewise, if the outbound traffic (OUT) is blocked, does that mean the web server request packet from the internal network is blocked?

When a web page is requested from a host in an internal network, that host sends a 'GET' request to the web server and the web server replies by returning an HTML file to the browser so that it can be displayed on the screen of the host. In this case, the initiative comes from the host on internal network and a request is sent outwards. This is outbound traffic. The reply comes from outside towards the internal network. This reply to the request is considered to be part of the same outbound connection. On the contrary, if someone from outside wants to connect to the internal web server of network, the outside host will send a 'GET' request to the internal web server. The connection is initiated from the outside, so this is an inbound connection. [16]

It can be misleading to interpret that a packet might appear to be inbound (IN) to the filtering device on its way to the external world, yet that packet is actually outbound (OUT) from the internal network. Thus, by using a simple terminology of TO (to replace IN) and FROM (to replace OUT), it can help the players to interpret the filtering rules more conveniently, as the player shall interpret the specific application service request as From/To the selected network. The change in the GUI's labeling, as shown in Figure 10, makes it much easier to interpret the directional traffic (i.e., Web Server request is permitted TO the Internet and Web server request is denied FROM the Internet).

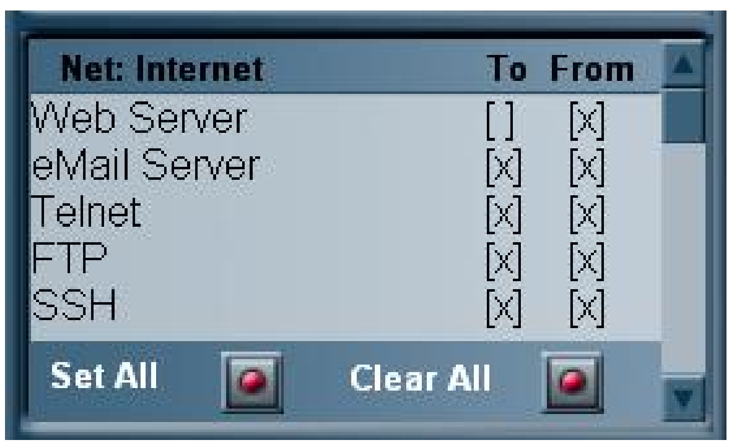


Figure 10 Interpretation of Rules

2. Packet Addressing

CyberCIEGE does not provide players with the means to specify filtering rules pertaining to source and destination of IP addresses.

3. Order of Rules

In CyberCIEGE, the matching of the rules in the filter devices does not concern the sequence or order of the rules. The underlying mechanism in the filter code will check

all the entries specified by the player. CyberCIEGE rules only contain application services. Therefore, the order of the rules is immaterial.

4. Static or Dynamic filtering mechanism

As described in Chapter II Section B, Comparison between Static and Dynamic Packet Filtering, the main significant difference between the two kinds of packet filtering is the awareness of connection state. The experimental results obtained in Table 1 and Table 2 are unable to prove that the filtering in CyberCIEGE has the ability to remember the directional flow of the packets.

Thus, CyberCIEGE provides no means of distinguishing a static filter from a dynamic filter since its does not model the flow of discrete packets, but only models application services.

G. SUMMARY

This chapter gave a description of the existing scenarios that relate to filtering components and some possible ideas that can be introduced to the existing scenarios to make the filtering subjects more educational. A roadmap of what is expected to be achieved in the development of the scenarios was mentioned, and a strategy was described using CyberCIEGE elements to illustrate network filtering concepts. Details of the resulting scenario development will be covered in Chapter IV.

IV. SCENARIO DESCRIPTION

A. SCENARIOS OVERVIEW

Three scenarios were developed in this thesis that allow players or students to have a better understanding of information assurance with emphasis in the area of packet filtering. These three scenarios can be used to complement the existing *TirePly Filters* Scenario to form a filtering campaign [17]. In this way, the player will have a progressive learning cycle about packet filtering and will experience some of the possible security issues related to packet filtering firewalls.

1. Common Definition

The three scenarios developed have common definitions in the Scenario Development Tool (SDT) element. They are:

a. Environment

All the three scenarios are developed based on an office environment. The skills and knowledge acquired in the office filter scenarios are applicable to other contexts such as the military.

b. Secrecy

Secrecy is required in organizations where access to information is governed by regulation or necessity to different groups of people. The secrecy of the assets and the clearance of the users are categorized into three levels in these scenarios: secret, confidential, and unclassified. This hierarchical system of secrecy specifies which level of security clearance is allowed to handle what classification of data. Different levels of security clearance require different levels of background checks as shown in Table 3.

	Unclassified	**Confidential**	**Secret**
Initial Background Check	Low	Medium	High

Table 3 Secrecy Level

(1) Secret – High Level. This level is defined as the highest level of sensitivity of information or security clearance. Any compromise of this

information could result in severe damage to the reputation of the company, confidence of employees and financial issues for the company.

(2) Confidential – Moderate Level. Confidential is defined as information that is meant for the authorized staff in the organization. Only authorized employees are allowed to access it. No one in the public should be able to access it. Any compromise of the confidential information may have a negative impact on the confidence of employees and probably will result in some revenue loss for the company.

(3) Unclassified – Low Level. Unclassified is defined as assets having the lowest sensitivity of information and is meant for everyone, including the public. It does not require any protection.

d. Scenario Conditions

Two main conditions classes, namely *AssetToNetworkByFilterType* and *AssetToNetworkFilterCount*, are used to measure the actions carried out by the player. In all three scenarios, each scenario has its own set of condition classes.

(1) AssetToNetworkByFilterType.

This condition class is used to determine whether an asset can be accessed from the network using the specified application service.

(2) AssetToNetworkFilterCount.

This condition class is used to determine whether the number of application services able to access the asset from the network exceed the input value specified by the game developer. This input value represents the maximum number of application services available.

These conditions, together with a trigger mechanism, provide positive and negative feedback to the player.

e. Scenario Triggers

TickerTrigger, SpeakTrigger, WinTrigger, CashTrigger and SetPhase trigger classes are used to improve dialogue with the player for all three scenarios. The trigger mechanism is activated when a set of conditions is met. Definitions of each type of trigger class are described as follows:

TickerTrigger causes information to be displayed on the ticker that appears at the bottom of the game screen.

SpeakTrigger causes information to be displayed as if the users are speaking or thinking during the game.

WinTrigger is used to display game debriefing information after the player has successfully won the game.

CashTrigger causes the cash in the game to increase or decrease depending on the player's success in fulfilling the user's goals.

SetPhase allows the player to advance the game to the next level. It also displays a new set of objectives for the player when the player has successfully completed a phase.

The trigger classes that are used in each scenario were tabulated. The tables give a general description of the conditions of when the trigger would occur and what messages would the player expect to receive.

B. SCENARIO 1: UNDERSTANDING PACKET FILTERING

In Scenario 1, the objective of the game is to introduce the player to packet filtering. By the end of this scenario, the players should be able to understand how the filter rules affect each of the application services.

1. Story Board

This scenario illustrates an automobile company. The following is the introductory message seen by the player.

Great Car Automobile, has decided to connect their internal network to the Internet. The main purpose is to generate a new source of revenue through the web. A fresh IT graduate was employed as an administrator to set up and maintain the Internet connectivity to the Great Car network. Within a week of the Internet connection, the internal network suffered from several attacks. Unskilled hackers from the Internet were the main suspects. Although the attacks were from amateurs, the consequences were detrimental. The work that was not backed up before the attack was lost. On top of that, the company had to suspend operations for two days to restore their backup information. As a result, an estimated loss of about US$ 50,000 was incurred. As the network was down, the company staff could not access the technical and financial records needed to

serve the customers. Several customers were unhappy because they had to reschedule their appointments for their vehicle maintenance.

The IT administrator was immediately instructed by management to disconnect the internal network from the Internet to prevent any further attacks. The IT administrator was dismissed and a new IT administrator was engaged.

In this scenario, the player is the new chief of the IT department. The player must apply the knowledge acquired on the topic of firewalls from an introductory computer security course to resolve some of the security issues.

The player needs to demonstrate his or her understanding of the use of packet filtering firewalls or routers. The organization has two sections: the Engineering department and Documentation department.

2. Assets

'Firebird' and 'Technical Manual' are the two information assets introduced in this scenario. Brief descriptions of the assets are described below in Table 2:

Asset Name	Secrecy Level	Description
Firebird	Secret	*It contains the company's intellectual property, technologies, and new ideas that have not been publicized. Anyone in the automobile industry would be keen to get a hold of this information. The company foresees that the information has potential value to bring in a new source of income that would sustain the company for the next five years according to its business roadmap. Any compromise of asset Firebird will not allow the company to survive for more than one year.*
Technical Manual	Confidential	*This information is important to the internal staff, especially to the mechanical engineering departments. This information provides specifications of automobile parts, guidelines on how to troubleshoot any mechanical defects and instructions to repair any faults in the hardware parts.*

Table 4 Scenario 1 Asset

3. Goal

Two goals were defined in this scenario. Each asset goal is assigned to each user as described in Table 5.

Asset Goal Name	Description
Update Technical Manual Goal	*The goal is to access the asset Technical Manual. This is essential to allow the accessibility and maintenance of the Technical Manual.*
Read Technical Manual Goal	*The goal is to access the Technical Manual over a network using a Database application service.*

Table 5 Scenario 1 Goal

4. Physical Component and Network

Two workstations, two networks and one firewall are used in the scenario. Each workstation is located in one of the networks, and both networks are connected using the firewall, as shown in Figure 11. Each workstation is assigned to one user and an asset is instantiated when the game starts. In the game, Joe's workstation/PC resides on LAN 1 and Jean's workstation/PC resides on LAN 2. Both workstations are connected to the router/firewall that allows some form of access control.

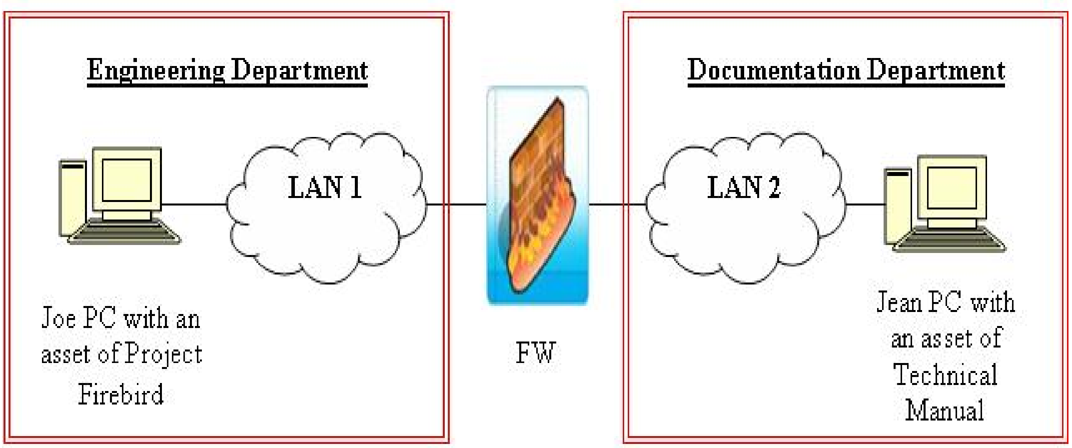


Figure 11 Scenario 1 Topology

5. Users

Two users, Joe and Jean, are created for this scenario, as shown in Figure 12.

Jean

Joe

Figure 12 Scenario 1 Users

Joe is a capable engineer from the Mechanical Engineering department. The company is pleased with Joe's performance and he was given a pay raise in the recent salary adjustment. Joe is very enthusiastic in his work and willing to take on new challenges. Joe is assigned to handle Project Firebird. He has the detailed information about Project Firebird in his workstation. He has been cleared with a secrecy level of Secret.

Joe's asset goal is to access the Technical Manual over a network using a Database application service. He needs the Technical Manual information for his engineering work.

Jean is a technical writer from the Documentation department. She is currently working alone as her peers have quit. She is responsible for all the technical specification documentation in the company. The Technical Manual resides in her workstation. Lately, she has been complaining that her workload is too much. The company has assured her that two more technical writers will be hired to help her out. Although Jean is a very hardworking employee, she is upset with her workload.

Jean's asset goal is to ensure that the Technical Manual information is updated to the current specification.

6. Filter

One filter entity is used in this scenario. The filter is labeled as 'CoFilter', and it is in the firewall component. Initially, the filtering rules are not setup properly. All the application services are blocked "From" and "To" network LAN 1 except for the "To" field of the Database application service. This improper filter allows Jean unauthorized access to Project Firebird. Joe, on the other hand, is unable to access the Technical Manual.

7. Full Briefing

In this scenario, a brief summary of the organization's network problem is described in the GAME tab as follows:

The filtering rule in the router/firewall was not properly setup. Jean seems to know about the details of Project Firebird while Joe is unable to retrieve information in the Technical Manual. The Technical Manual can be accessed through the DATABASE application.

Firewalls inspect packets as they pass through, and based on the rules that the administrator has defined, they allow or deny each packet through the firewall. Communication between computers requires packets to be sent and received in both directions. From the firewall's perspective, the distinction between "inbound" and "outbound" connections is the direction of the first packet which begins the exchange (also known as Initial Request Packet). When a particular network is selected, one can deny or permit the initial request packet to flow TO or FROM that network.

In this case, one cannot completely seal off LAN 1 from LAN 2, but one does not want this opening to be used by anyone from LAN 2 to exploit the LAN 1 network. One can either configure the filtering rules on the LAN 1 or LAN 2 interface of the filtering device to give the same effect.

On the "TO" column, it is interpreted as a Permit/Deny Initial Request Packet TO the selected network.

For the "FROM" column, it is interpreted as a Permit/Deny Initial Request Packet FROM the selected network.

8. Conditions

A set of conditions are used to measure the actions carried out by the player. The conditions, together with a trigger mechanism, provide positive and negative feedback to the player.

a. AssetToNetworkByFilterType

Table 6 shows the AssetToNetworkByFilterType condition class that was used in Scenario 1. For example, 'JoeAccessHacker' is a condition that will return with a

Boolean ('TRUE' or 'FALSE') value that indicates whether the asset **Technical Manual** can be accessed from network **LAN 1** using the **Database** application service.

Condition Name	Asset	Network	Application Service
JoeAccessHacker	Technical Manual	LAN 1	Database
JeanAccessJoe	Firebird	LAN 2	Database

Table 6 Scenario 1 AssetToNetworkByFilterType

b. AssetToNetworkFilterCount

Table 7 shows a set of AssetToNetworkFilterCount condition class that was used in Scenario 1. For example, 'BlockServices_From' is a condition that returns 'TRUE' when more than **one** application service type can access the **Technical Manual asset** from network **LAN 1**.

Condition Name	Count	Asset	Network
BlockServices_To	0	Firebird	LAN 2
BlockServices_From	1	Technical Manual	LAN 1

Table 7 Scenario 1 AssetToNetworkFilterCount

9. Trigger Mechanisms

In the scenario, TickerTrigger, SpeakTrigger, WinTrigger and CashTrigger triggers are used to improve dialogue with the player. The trigger mechanism is activated when a set of conditions is met as described in the Tables 8, 9, 10 and 11.

a. TickerTrigger

Table 8 shows a list of *TicketTrigger* that are used in the Scenario 1.

Trigger Name	Triggered Conditions and Messages
MsgTickerHackerAccessJoe	Jean is able to access Project Firebird. *It is usual that Jean is downloading large files from LAN 1.*
MsgTickerExcessOpening	More than zero application services are allowed to LAN 1. *There are unnecessary applications services allowed TO the LAN 1.*

Trigger Name	Triggered Conditions and Messages
MsgTickerJoeAccessHacker	All user goals and objectives are met. *Great! You have successfully protected the Project Firebird using the filtering rule.*
JoeNoAccessTechManual	Joe is unable to access Technical Manual. *Joe can't access Technical Manual.*
TightenSecurityTicker_From	Joe is able to access Technical Manual and there are other application services not blocked. *Is Filter Database application service "FROM" not properly configured?*
TightenSecurityTicker_To	Joe is able to access Technical Manual and Jean is able to access the Project Firebird. *Is Filter Database application service "TO" not properly configured?*

Table 8 Scenario 1 TickerTrigger

b. SpeakTrigger

These triggers served as a form of feedback to the players, as described in Table 9.

Trigger Name	Triggered Conditions and Messages
HackerClaim	Jean is able to access the Project Firebird. *Joe PC has so much information. Seems to worth a lot of money.*
ThoughtTriggerJoe	Jean is able to access the Project Firebird. *Why is my computer so slow? It seems that someone is accessing my computer.*

Table 9 Scenario 1 SpeakerTrigger

c. WinTrigger

Table 10 describes the debrief messages for Scenario 1 when the player has successfully won the game.

Trigger Name	Triggered Conditions and Messages
ScenarioCompleted	All objectives are met. All unused application services are denied and Joe is able to access the asset Technical Manual. *Great! By now you should have a clear understanding of*

	how the filtering rules work in CyberCIEGE. It is based on the concept of stateful packet filtering whereby when a filter is configured to permit a traffic request, the filter allows traffic that is associated with the permitted request to pass. Ideally, you need to know exactly what services you expect from the clients before you can restrict your firewall accordingly.

Table 10 WinTrigger

d. CashTrigger

Descriptions of CashTrigger triggers that are used in Scenario 1 are described in Table 11.

Trigger Name	Triggered Conditions	Amount
CashLostJeanAccess Joe	Jean is able to access the Project Firebird.	- $100
CashLostJoeGoalFail	Joe is unable to access Technical Manual.	- $500
CashLostTooManyServices	More than 0 application services can access Firebird from LAN 2 or more than 1 application services can access Technical Manual from LAN 1.	- $1000
CashIncrease	All objectives are met.	+ $100

Table 11 Scenario 1 CashTrigger

10. Objective and Phases

In this scenario, there is only one objective and one phase. The objective of the phase is to educate the player to be able to interpret the filter configuration table and understand how it should be configured. The game is only completed when the player correctly sets the filtering rules such that the Database application service is able to access information in LAN 2 from LAN 1 and all application services are denied from LAN 2 to LAN 1. If the objective is not met, cash will be deducted according to the severity of the outcome affected by the filtering rules by CashTrigger. Details of the phase and objective are described in Table 12 and Table 13.

Field Name	Description
Phase Name	Phase0
Display Name	*Understand filter rules*
Completed Text	*Done.*
Uncompleted Text	*Setup the filter rules such that Joe can access the Technical Manual*

	using the Database application service and only Joe can access the Project Firebird.

Table 12 Scenario 1 Phase 0 Detail

Field Name	**Description**
Objective Name	FilterObj0
Phase	0
Uncompleted Text	*You can focus on the Database application service and any one Firewall interface, e.g. LAN1. Each time you make changes to the rules that affect the Database application service, go to the USER tab and observe whether you have successfully accomplished the goal for each user.*

Table 13 Scenario 1 Objective Detail

C. SCENARIO 2: IP SPOOFING AND APPLICATION SERVICES

In the second scenario, the complexity of filtering is extended to handle a network connection to the Internet. The main focus of this scenario is to introduce the IP spoofing issue and what to do with any unused application services when connecting to the Internet.

As discussed in Chapter III, players should always deny any traffic from the Internet when the "from address" corresponds to an IP address in the internal network. The same principles apply to block anyone from the internal network from spoofing an external network intentionally or otherwise. The player will also learn to take a proactive approach by blocking all application services from the Internet. Any request for services should be reviewed by the administrator and approved by management.

1. Storyboard

In Scenario 2, the introduction is described as follows:

Great Car Automobile has expanded their enterprise. A production plant was setup away from headquarters office. In the production plant, there is an internal network which is connected to the Internet for its employees to surf the web. In the headquarters office, both the Engineering and Financial departments require Internet access. The engineers need the Internet to do their research studies. The accountants in the Financial department need the Internet to monitor currency trading. However, the

management of Great Car Automobile is concerned about leakage of their trade secret Project Firebird information and accounts records. Any compromise of these assets could result in the company losing a great deal of money as well as tarnishing its reputation.

Since management knows that the Internet is necessary for their business, they have instructed the IT administrator to look into this matter. The management has emphasized that they will not purchase any new network equipment. The IT administrator has to use the existing equipment such as the firewall device to protect the company's assets and allow connectivity to the Internet.

2. Asset

'Project Firebird', 'Account Book' and 'WebAsset' are the three information assets introduced in this scenario. Project Firebird in this scenario is the same as the asset that is described in Scenario 1. It is reused in this scenario. Brief descriptions of the 'Account Book' and 'WebAsset' are described as follows in Table 14:

Asset Name	Secrecy Level	Description
WebAsset	Unclassified	*This information can be accessed by anyone in the organization and the public on the Internet.*
Account Book	Secret	*It resides in the headquarter office. It contains sensitive information such as the company's financial situation and detailed information about its financial transactions. It should not be accessible to any unauthorized personnel.*

Table 14 Scenario 2 Assets

3. Goal

Two goals were defined in Scenario 2 as shown in Table 15.

Asset Goal Name	Description
Web Goal	*The goal is to access the asset 'WebAsset' using Web Server software.*
Firebird Goal	*The goal is to access the asset 'Project Firebird' using Database application service.*

Table 15 Scenario 2 Goals

4. Physical Components and Networks

Three workstations, one server, three internal networks, one Internet and two firewalls are used in the scenario.

In the headquarters office, there are two internal networks, LAN 1 and LAN 2, which are connected to a firewall, named CoFilter. There is one workstation in each of the networks and both networks are connected using the firewall. Each workstation is assigned to one user and an asset is instantiated upon the start of the game. In the game, Joe's workstation/PC resides on LAN 1 and Mary's workstation/PC resides on LAN 2. The headquarters office is not connected to the Internet. See Figure 13.

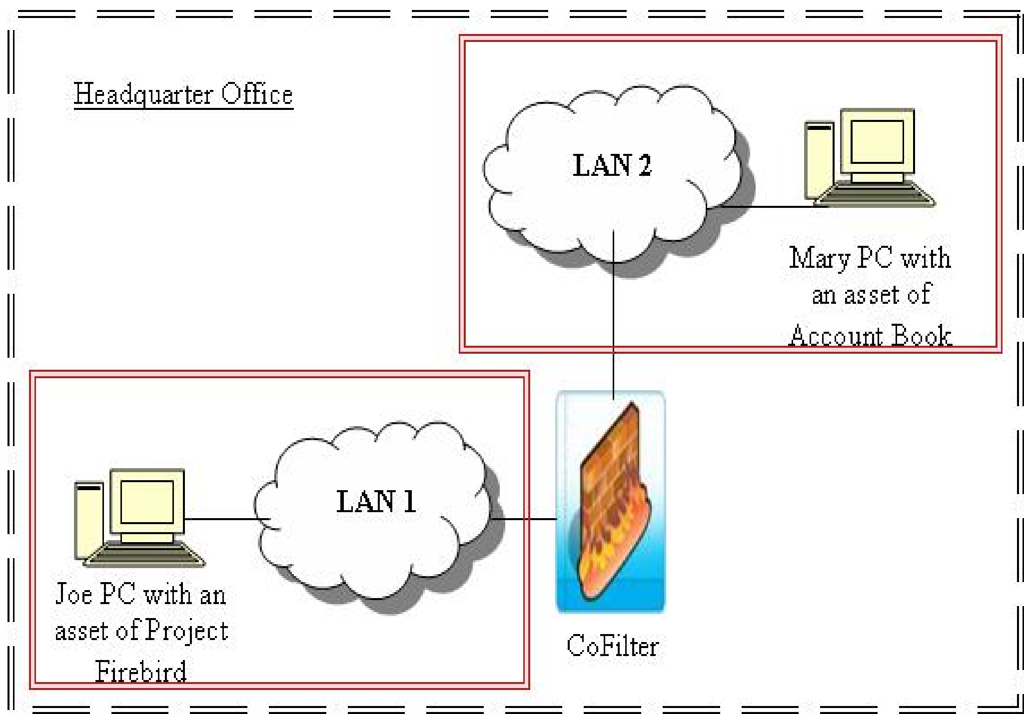


Figure 13 Scenario 2 Headquarter Topology

At the remote site, a production plant, a simple network with Internet connectivity is established as shown in Figure 14. A Web Server and Henry's PC are connected on LAN 3 and an asset named WebAsset is instantiated on Web Server when the game starts.

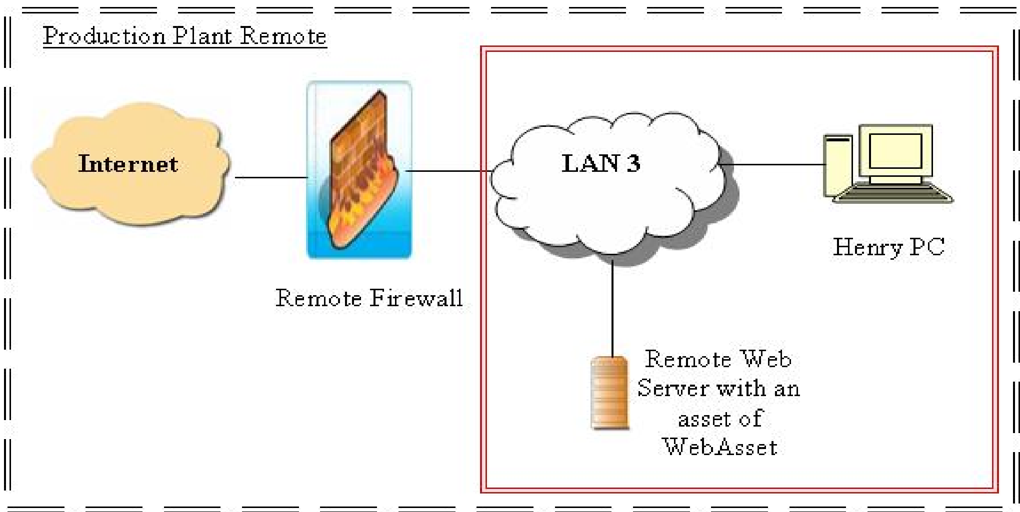


Figure 14 Scenario 2 Remote Production Plant

5. Users

Joe has the same role as in Scenario 1. The descriptions of the users, as seen in the scenario, are given below.

Joe's asset goals are 'Web Goal' and 'Firebird Goal'. Joe has to access the Internet to do his research for the Project Firebird. Joe requires Internet research to generate a list of material for the project.

Mary is an accountant who works in the Finance department. She has been working for the company for fifteen years and has been very loyal. She has a secrecy level of Secret. She is in charge of important information namely the Account Book. Her asset goals are 'Web Goal' and 'Firebird Goal'. She needs to access the Internet to compute expenses and monitor the budget for Project Firebird. On top of that, she has to access Project Firebird and the Internet to generate a list of raw materials for Project Firebird. The list of materials may then be used for an on-line reverse auction on the Internet.

Henry joined the company less than two months ago and he is under probation. He is recruited as a production worker in the remote production plant. His asset goal is 'Web Goal'. Although there are many production orders to be carried out, Henry seems to have plenty of time to surf the web. Henry has downloaded free hacking kits from the

web. He is trying out his new found toys on company computers. Henry happens to know one of the internal IP addresses of the headquarter office.

6. Filter

The filtering configuration on the two firewalls that are installed at the headquarters office and production plant, are reset to their defaults. By default, no application services are blocked.

7. Full Briefing

When the Internet has been connected to the internal network at the headquarters office, a regular analysis on the firewall log is carried out weekly. From the analysis report, it seems that there is traffic from the Internet, using an internal IP address as a source IP address.

A port scan is carried out from the headquarters office and the report shows that there are many application services that can be exploited.

Firewalls filter traffic based on their protocol, sending or receiving port and IP addresses or values of some status bits in the packet. Regardless of the types of filter being used, it is essential to block any incoming traffic that has an IP address that matches one's internal network addresses.

A rule of thumb is to deny all traffic/application services unless they are specifically requested. Remember that any application services that one leaves open, which is not used can potentially benefit hackers, viruses and worms.

8. Conditions

A set of conditions are used to measure the actions carried out by the player. The conditions are used with trigger mechanisms to provide positive and negative feedback to the players.

In this scenario, at the network LAN 1, the Web Server application service is allowed to access the WebAsset. At the network LAN 2, the Web Server application service is allowed to access WebAsset and the Database application service is allowed to access Project Firebird. The following conditions as shown in Table 16 and Table 17 are implemented to measure the player's performance in the game.

a. AssetToNetworkByFilterCount

For example, ’FW2PortFromOpen’ is a condition that returns ‘TRUE’ when more than **two** application service types can access the **Project Firebird asset** from the **Internet**.

Condition Name	Count	Asset	Network
FW2PortFromOpen	2	Project Firebird	Internet
FWOpenPortFromInternetToLan1	0	Project Firebird	Internet
FWOpenPortFromLan2ToInternet	1	WebAsset	LAN2
FWOpenPortFromLan1ToInternet	1	WebAsset	LAN1
FWOpenPortFromLan1ToLan2	0	Account Book	LAN 2
FWOpenPortFromLan2ToLan1	1	Project Firebird	LAN 2
FWOpenPortFromInternetToLan2	0	Account Book	Internet

Table 16 Scenario 2 AssetToNetworkByFilterCount

b. AssetToNetworkByFilterType

For example, ’JoeAccessFinancialAccount’ is a condition that will return with a Boolean (‘TRUE’ or ‘FALSE’) value that indicates whether the asset **Account Book** can be accessed from network **LAN 1** using the **Database** application service.

Condition Name	Asset	Network	Application Service
JoeAccessFinancialAccount	Account Book	LAN 1	Database
JoeAccessInternet	WebAsset	LAN 1	Web Server
MaryAccessProjectFirebird	Project Firebird	LAN 2	Database
MaryAccessInternet	WebAsset	LAN 2	Web Server
HenryAccessProjectFirebird	Project Firebird	Internet	Internal IP Address
HenryAccessFinancialAccount	Account Book	Internet	Internal IP Address

Table 17 Scenario 2 AssetToNetoworkByFilterType

9. Trigger Mechanisms

The trigger mechanisms are implemented to provide feedback to the player that there are necessary actions to be carried out before an attack occurs. Tables 18 through Table 23 provide the descriptions of the trigger mechanisms implemented in this scenario.

Trigger Name	Triggered Conditions and Messages
SpeakerTriggerJoe0	Joe is unable to access the WebAsset in Phase 0. *Is there a problem with the Internet?*
SpeakerTriggerMary0	Mary is unable to access the WebAsset in Phase 0. *Why can't I access the Internet?*
SpoofingJoeHost	Henry is able to use Internal IP address application services to access the assets on Project Firebird or Account Book in Phase 1. *Why is my system so slow? Why am I getting these funny messages?*
SpoofingMaryHost	There is ongoing IP spoofing. *Why is my system so slow?*
SpeakerTriggerMary2	Mary is unable to access the Project Firebird in Phase 2. *I need to access Project Firebird.*

Table 18 Scenario 2 SpeakerTrigger

Trigger Name	Triggered Conditions and Messages
SetPhase0Completed	Joe and Mary are able to access the WebAsset in Phase 1. *Great. Joe and Mary are happy to have Internet access again. See Next Objective.*
SetPhase1Completed	Henry is unable to access Project Firebird and Account Book and both Joe and Mary are able to access WebAsset in Phase 1. *You have successfully prevented anyone from the Internet to spoof your internal network.*

Table 19 Scenario 2 SetPhase

Trigger Name	Triggered Conditions and Messages
InternalLanExploitation	The filtering rules are incorrect. *Filter Rules between LAN 1 and LAN 2 are incorrect.*
TickerMsgIPSpoofing	Henry is able to access Project Firebird asset and Account Book in Phase 1. *Firewall log review shows that there are internal IP spoofing incidents.*

Table 20 Scenario 2 TickerTrigger

Trigger Name	Triggered Conditions and Messages
AccessInternetP1	Joe and Mary are unable to access the WebAsset in Phase 1. *Joe and Mary still need Internet access.*

Table 21 Scenario 2 MessageTrigger

Trigger Name	Triggered Conditions and Messages
WinGame	All user goals and objectives are met. *You have successfully completed Scenario 2. Go to Scenario 3 for more challenges.*

Table 22 Scenario 2 WinTrigger

Trigger Name	Triggered Conditions and Messages	Amount
P0CashLost	Jean or Joe or Both is unable to access the Internet in Phase 0.	- $100
P0CashWin	Both Jean and Joe can access the Internet in Phase 0.	+$100
P1CashLost	Project Firebird and Technical Manual is accessed by someone from the Internet	- $2000
P2CashLostNoInternetAccess	Joe or Mary or Both has no Internet Access in Phase 2. *Joe and Mary still need Internet access.*	-$250
P2CashLostTooManyServices	Excessive application services available to employees and public. *Exploitation of application services.*	-$1000

Table 23 Scenario 2 CashTrigger

10. Objectives and Phases

In this scenario, there are three objectives and three phases. In Phase 0 (Internet Access), the objective is to allow both Mary and Joe to have Internet access.

Joe requires Internet access to do his web research. Mary needs to have on-line web access to get details on currency exchange rates, reverse auctions and e-banking.

Top management has given their approval that both Joe and Mary shall be given access to the Internet. It is required that this request be attended to.

In Phase 1 (IP Spoofing), the objective is to ensure that the filter is setup to block any traffic from the Internet that is using any of the IP address of its internal network.

Complaints have been received from staff in the company claiming that the network is very slow and unstable. The firewall logs have been analyzed and there is a lot of traffic coming from the Internet pretending to be one of the internal network addresses.

One can setup a "Spoofing filter" on the firewall - Don't allow traffic from the Internet that indicates a source IP address matching any of the internal network addresses. This keeps attackers from "Spoofing" the machines.

In Phase 2 (Port Scanning), the objective is to ensure that the filter is setup to allow Mary access to both the Internet and Project Firebird information and Joe is able to access the Internet. Remaining application services that are not specifically permitted should be denied.

Recently, a port scan security check was conducted on the network. The test results show that there are risks that the network might be exposed to due to unnecessary application services. If the services are not necessary, they should be shut down or blocked.

The general rule of thumb is to deny access to everything except for common services such as web servers, e-mail, etc and then allow other types of traffic to pass through upon request. The basic idea is to start with a restrictive policy then expand the list of permitted services as needed.

Rule 1) Allow Joe to have Internet access using the Web Server.

Rule 2) Allow Mary to have Internet access using the Web Server.

Rule 3) Allow Mary to access the information of Project Fireball and to compile the project budget by using the Database application.

Upon completion of the three phases, the player is said to have successfully completed Scenario 2.

D. SCENARIO 3: DEMILITARIZED ZONE (DMZ)

In the third scenario, the level of difficulty of the game has been increased. This is done by increasing the number of servers and networks. However, the basic understanding of packet filtering still applies. With an increase in complexity of the network topology, now the focus of the game is to address the IP spoofing, deny any unused application services when connecting to the Internet, and placement of any public servers in a DMZ.

1. Storyboard

The following is the introductory message of scenario 3:

Great Car Automobile has expanded its business. They decided to have their own web server as well as FTP download and upload area. The public is allowed to access the company web pages and FTP download and upload area while the remaining assets such as Project Firebird and Financial Accounts information should remain properly secured. The employees are also allowed to access the company Web Server and FTP server.

Company management has reviewed the previous proposed solution to protect the internal network. They have given the "green light" to proceed to implement a DMZ solution. The current topology needs to be studied and the amount of change needs to be minimized so as to reduce the impact of disruption on the employees.

2. Asset

'Public FTP Data', 'Public Web Pages Data', 'Group Ware Data', 'IntraNet Data', 'Firebird Data', 'Financial Account Data' and 'RemoteWebAsset' are the information assets introduced in this scenario. Firebird Data and Financial Account Data

are the same assets as described in Scenario 2. They are reused in this scenario. Public FTP Data, Public Web Pages Data, Group Ware Data and IntraNet Data are described in Table 24 as follows:

Asset Name	**Secrecy Level**	**Description**
RemoteWebAsset	Unclassified	*This information can be accessed by anyone in the organization and by the public from the Internet. It resides on the Remote Web Server at the Production Plant. This can be accessed by using the Web Server application service.*
Public FTP Data	Unclassified	*Information uploaded or downloaded by public users and employees. This information resides on 'Public FTP Server' which can be accessed via the FTP application service.*
Public Web Pages Data	Unclassified	*Information published by the company creates interaction with Internet users and establishes e-commerce business. This information is stored on the 'Public Web Server', which can be accessed using the Web Server application service.*
Group Ware Data	Confidential	*Tools and software applications help communication and information sharing and promote collaboration among staff and colleagues by allowing users access to their email, plans and share documents. This information should only be accessible by employees of the company. It resides on 'Private GroupWare Server' and is only accessible by using the Database application service.*
IntraNet Data	Confidential	*This information could include data from manufacturing, payroll, human resources, research and development, marketing, and engineering. This data is critical to business operations. Thus, this information should only be accessible to employees. They are stored in 'Private IntraNet Server' and can be accessed via Management application service.*

Table 24 Scenario 3 Assets Details

3. Goal

Five goals were defined in Scenario 3 as shown in Table 25.

Asset Goal Name	**Description**
Internet Goal	*The goal is to access the asset 'WebAsset' using the Web Server application. Internet access is needed for research, foreign currency exchange rates and on-line auction.*
FTP Goal	*This goal is to access the FTP uploading and downloading data area. This area contains information required by the employees and the public.*
Company Web Pages Goal	*This goal is to access the Company's publicity web pages and conduct e-business.*
IntraNet Goal	*This goal is to access IntraNet Data which are sensitive. It is restricted to its internal employees.*
GroupWare Goal	*This goal is to access the GroupWare Data which allows communication services to be available. It should not be accessed by outsiders.*

Table 25 Scenario 3 Goals

4. Physical Component and Network

Two workstations, five servers, three internal networks, one Internet and three firewalls are used in Scenario 3. In this scenario, the 'Public Web Server' and 'Public FTP Server' are not connected to the internal network as shown in Figure 15. LAN 1, LAN 2, 'Private IntraNet Server', 'Private GroupWare Server' and Mary's and Joe's workstations are setup as static so that conditions and triggers can be used to measure the effectiveness of the player throughout the game. The setup of the production plant is static as shown in Figure 16.

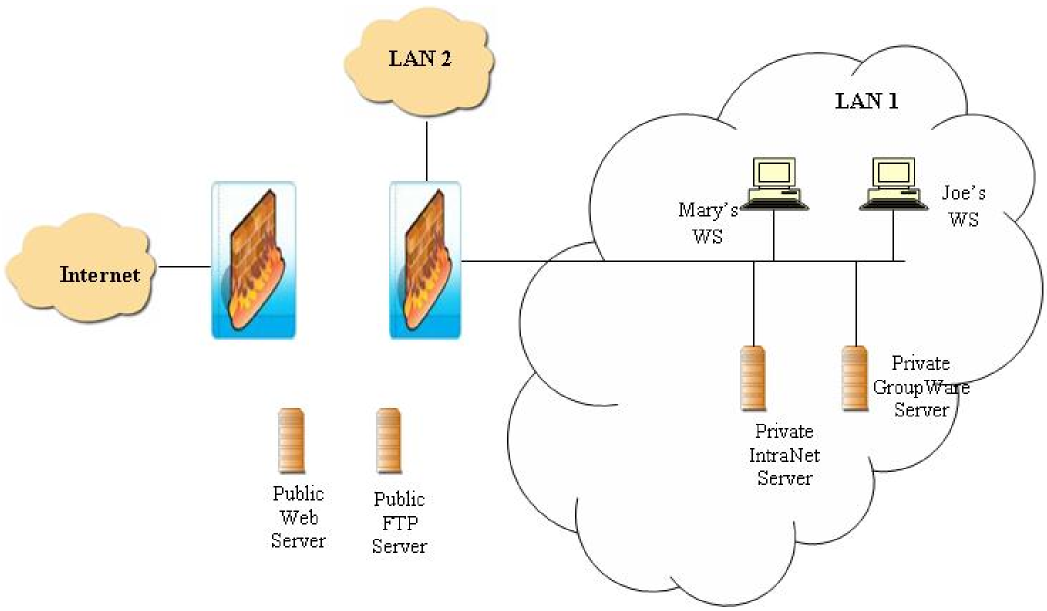


Figure 15 Scenario 3 Initial Headquarter Office Setup

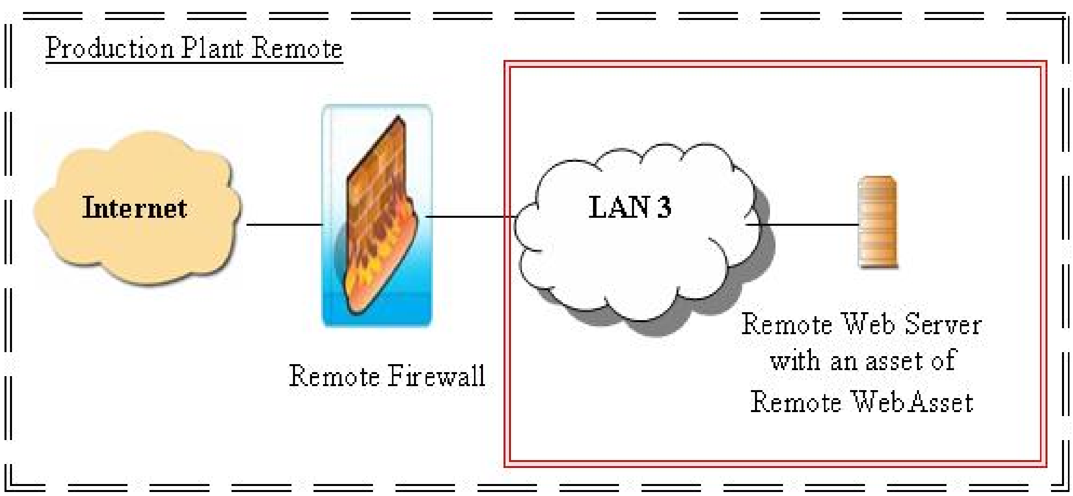


Figure 16 Scenario 3 Production Plant

5. Users

In Scenario 3, there are two users namely Joe and Mary. They play the same role as in Scenario 2. Both Joe and Mary have the following multiple asset goals:

- To have 'RemoteWebAsset' reside on the 'Remote Web Server' using the Web Server application service.
- To have 'Public FTP Data' reside on the 'FTP server' using the FTP application service.

- To have ‘Public Web Pages Data’ reside on the ‘Web Server’ using the Web Server application service.
- To have ‘IntraNet Data’ reside on the ‘IntraNet Server’ using the Database application service.
- To have ‘Group Ware Data’ reside on the ‘GroupWare Server’ using the Management application service.

6. Full Briefing

With the realization of e-business, public users are able to access the enterprise’s public Web Server. The public can also upload and download files to/from the public FTP server. However, they should not be allowed to access the company’s private servers. Employees of the company are allowed to access both the public servers and private servers but they are restricted from using the FTP application services outside the Internet. The employees also need to access the remote web pages that are located on the remote Web Servers.

The idea of a DMZ is a small network implemented in the neutral zone between the company's private network and the public network. It prevents outside/public users from getting direct access to a server or workstation that has valuable company data. Public users outside the company’s network can access only the devices in the DMZ. Typically, a DMZ may allow the company's web servers to be of service to the outside world but accessibility by the public to the company private data is restricted. In the event of any host compromise in the DMZ, such as the compromise of information on the web servers, no other company information will be vulnerable.

7. Conditions

The Project Firebird and the Financial Account Data reside on LAN 1. Two application services (FTP and Web Server) can be used to access the assets on the private servers from the Internet. One application service (Web Server) is allowed to access the RemoteWebAsset from LAN 1. Two application services (FTP and Web Server) are allowed to access the private servers from LAN 1. The conditions are shown in Table 26 and Table 27.

a. AssetToNetworkByFilterCount

An example from Table 26 is 'FW1OpenPortTo', which is a condition that returns 'TRUE' when more than **one** application service type can access the **Public Web Pages Data asset** from network **Internet**.

Condition Name	Count	Asset	Network
FW1OpenPortTo	1	Public Web Pages Data	Internet
FW1OpenPortFrom	2	Public FTP Data	Internet

Table 26 Scenario 3 AssetToNetworkByFilterCount

b. AssetToNetworkByFilterType

An example from Table 27 is 'JoeAccessRemoteWebAsset', which is a condition that will return with a Boolean ('TRUE' or 'FALSE') value that indicates whether the asset **RemoteWebAsset** can be accessed from network **LAN 1** using the **Web Server** application service.

Condition Name	Asset	Network	Application Service
JoeAccessRemoteWebAsset	RemoteWeb Asset	LAN 1	Web Server
MaryAccessRemoteWebAsset	RemoteWeb Asset	LAN 1	Web Server
SpoofInternalIP	Firebird Data	Internet	Internal IP address
ReachPublicFTP_Server	Public FTP Data	Internet	FTP
ReachPublicWeb_Server	Public Web Pages Data	Internet	Web Server
EmployeeAccessPublicWeb_Server	Public Web Pages Data	LAN 1	Web Server
EmployeeAccessPublicFTP_Server	Public Web Pages Data	LAN 1	FTP
ReachPrivateGroupWare_Server	Group Ware Data	Internet	Web Server
ReachPrivateIntraNet_Server	Group Ware Data	Internet	Web Server

Condition Name	Asset	Network	Application Service
StealPrivateIntraNet_Server_WebServer	IntraNet Data	Internet	Web Server
StealPrivateIntraNet_Server_FTP	IntraNet Data	Internet	FTP
StealPrivateGroupWare_Server_FTP	Group Ware Data	Internet	Web Server
StealPrivateGroupWare_Server_WebServer	Group Ware Data	Internet	Web Server
StealPrivateServerData_ByFTP	IntraNet Data	Internet	FTP
StealPrivateServerData_ByWebServer	IntraNet Data	Internet	Web Server

Table 27 Scenario 3 AssetToNetworkByFilterType

8. Trigger

Tables 28 to Table 33 show listings of different classes of triggers that are implemented in Scenario 3.

Trigger Name	Triggered Conditions and Messages
Joe_NoInternet	Joe is unable to access the WebAsset in Phase 0. *What's wrong with the Internet? I can't do my Internet Research!*
Mary_NoInternet	Mary is unable to access the WebAsset in Phase 0. *Why can't I access the Internet?*

Table 28 Scenario 3 SpeakTrigger

Trigger Name	Triggered Conditions and Messages
SetPhase0Completed	Employees are able to access the Internet and Public Servers in Phase 0. *Well Done! Joe and Mary are able to access the Internet and Public Servers. See the Next Objective.*
SetPhase1Completed	No Internal IP spoofing and employees are able to access Internet and public servers in Phase 1. *Great! It is important to block any traffic that spoof your internal network.*

Table 29 Scenario 3 SetPhase

Trigger Name	**Triggered Conditions and Messages**
Both_NoInternet	Employees cannot access the WebAsset in Phase 0. *Both Joe and Mary are upset, they can’t access the Internet.*
Both_NoPublicServer	Employees cannot access assets on public servers in Phase 0. *Employees can’t access the public servers.*
Both_NoFTPServer	Employees cannot access FTP server in Phase 0. *Employees can’t access the Public FTP Server.*
Both_NoPublicWebServer	Employees cannot access the ‘Public Web Server’ in Phase 0. *Employees can’t access the Public Web Server.*
InternalIPSpoof	Someone is spoofing the Internal IP address from the Internet in Phase 1. *Is your network vulnerable to internal IP spoofing?*
FW1CheckFrom	Too many application services are open to the Internet in Phase 1. *Are there too many application services available to public?*
No_Internet	Joe and Mary cannot access the Internet in Phase 1. *Joe and Mary can’t access the Internet*
No_PublicServer	Public servers cannot be accessed by the public in Phase 1. *Public Servers are not available to the public.*
FW1CheckTo	Too many application services are available for employees in Phase 1. *Joe is exporting other application services to the Internet.*
EmployeeNoPublicWebServer	Employees cannot access public web servers in Phase 2. *Joe and Mary need to access the Public Web Server.*
EmployeeNoPublicServer	Employees have no access to public servers in Phase 2. *Joe and Mary cannot access the public servers.*
EmployeeNoPublicFTPServer	Employees cannot access Public FTP Server in Phase 2.

Trigger Name	Triggered Conditions and Messages
	Joe and Mary need access to the Public FTP Server.
GetIntraNetData	Someone from the Internet is accessing the IntraNet Data in Phase 2. *IntraNet server is vulnerable to attacks.*
GetPrivateServerData	Someone from the Internet is accessing both the IntraNet Data and the Group Ware Data in Phase 2. *Malicious application services have sneaked onto the private servers and have destroyed information. Information on the servers has to be reinstalled.*
GetGroupWareData	Employees cannot access the Group Ware Data in Phase 2. *Joe and Mary have missed their deadline for proposal submission because they cannot access the GroupWare server.*

Table 30 Scenario 3 TickerMessage

Trigger Name	Triggered Conditions and Messages
AccessInternetP1	Joe and Mary are unable to access the WebAsset in Phase 1.

Table 31 Scenario 3 MessageTrigger

Trigger Name	Triggered Conditions and Messages
WinGame	All user goals and objectives are met in Phase 2. No Internal IP spoofing, Employees have access to the Internet, private and public servers, and any unused application services are denied to employees and for public exploitation. *You have completed the Filter Campaign*

Table 32 Scenario 3 WinTrigger

Trigger Name	Triggered Conditions and Messages	Amount
LostCost	Employee unable to access Remote WebAsset or data on public servers.	- $100
FW_To_ManyOpenServices	Too many unnecessary application services available.	- $500
LostAttackPrivateServer	Public can access private servers. *Private servers being attacked.*	- $2500

Trigger Name	Triggered Conditions and Messages	Amount
LostCostIPSpoof	IP Spoofing on the internal network	- $1000

Table 33 Scenario 3 CashTrigger

9. Objective and Phase

In this scenario, there are three phases. In Phase 0 (Internet Access), the phase and objective are similar to the one in Scenario 2 except that the network topology is different as there are more servers and an additional firewall in the internal network. The objective is to allow both Mary and Joe to have Internet access and have access to the data on the public servers.

Joe requires Internet access to do his web research. Mary needs to have on-line web access to get details on currency exchange rates, reverse auctions and e-banking. Both Joe and Mary are required to access the public servers as well.

Top management has given their approval that both Joe and Mary shall be given access to the Internet. It is required that this request be attended to.

For Phase 1 (IP Spoofing and Port Scanning), the objective is to ensure that the filters are setup to block any traffic from the Internet that is using any of the IP addresses of its internal network. Public users should be able to access the public servers, namely Public Web Server with the Web Service application, and Public FTP Server with the FTP application. Employees are not allowed to use FTP application services to the Internet.

Port scanning was conducted regularly on the network. From the scanning results, there are many application services that can be exploited either by employees or malicious outsiders. The log files of the firewalls indicate that traffic from the Internet is spoofing the Internal IP address.

One can setup a "Spoofing filter" on the firewall that will deny traffic from the Internet when the source IP address matches any of your internal network addresses. If the associated application ports are not used, they should be shut them down or blocked. The public should only be permitted to access the public servers only.

In Phase 2 (DMZ), the objective is to ensure that the filters are setup to allow Mary and Joe to achieve their user goals. Public users from the Internet must be able to access the assets of Public Web Pages Data and FTP Data. Employees are not permitted to use FTP application services to access the Internet. To achieve the objectives of Phase 2, the network topology needs to be changed. A DMZ topology is a possible solution.

Access to public servers is required by both employees and the public. The private servers must not be accessed by the public. The employees need to access the Internet in order to carry out their work.

Rule 1) The public users and company employees are allowed to access the web pages and FTP data on the DMZ.

Rule 2) Employees are allowed to download information from the public FTP server.

Rule 3) Joe and Mary need to have Internet access.

Rule 4) All unused application services should not be left enabled so as to prevent exploitation by employees and the public.

E. SUMMARY

This chapter has provided a description of three scenarios on network filters. The users, assets, components, network topology, users' goals, conditions and trigger mechanisms that are used to implement each scenario are introduced. A brief introduction to each scenario is also presented. In the next chapter, test strategies and test cases will be described. It will also include the expected and actual test results.

V. TESTING

A. TEST STRATEGY

The goal of testing is to ensure that all three scenarios provide players with the appropriate feedback. The feedback provided to the players will include situations when the "correct" choices were made and also when mistakes were made. Testing for all the three scenarios is primarily to ensure that the player-visible triggered messages appear under selected conditions.

1. Test Development

Tests were developed in two stages. The first series of tests were done informally in support of scenario development. A second set of simple test cases with expected outcomes were developed during the implementation of the scenario. These test cases are unlikely to have covered all the possible aspects of the game. The second series of tests were more detailed. The test cases only considered what were thought to be the most likely moves the players would make, including mistakes.

This chapter describes the detailed testing that was performed on each phase.

2. Networks and Filters Rules

In the scenarios of this thesis, the player has two tasks: the first is to modify the network topologies, and the second is to set up the filtering rules. Therefore, the test cases were developed based on different network topologies and filtering rules as inputs to the games.

B. SCENARIO 1 TESTING

In the first scenario, the network topologies are static which means that LAN 1 and LAN 2 cannot be changed by the player. Therefore, the element of network topology variation can be ignored. The test was based on the different combination of filter rules. Table 1 is the legend used in the test cases in Scenario 1.

Symbol	Description
[ ]	Permit
[X]	Deny
[D]	Don't Care
T1	Ticker message: *"Great! You have successfully protected the Project Firebird using the filtering rule"*.
T2	Ticker message: *"It is unusual that Jean is downloading large file sizes from*

Symbol	Description
	LAN 1”.
T3	Ticker message: *“Joe can’t access Technical Manual”.*
	LAN 1
	LAN 2

Table 34 Scenario 1 Legend

1. Scenario 1 Overview

The objective of this scenario is to ensure that the asset ‘Technical Manual’, which resides on Jean’s PC, can be accessed by Joe from LAN 1 using the Database application service only. Therefore, tight filter rules on ‘CoFilter’ should only allow the Database application service request from LAN 1 to LAN 2. Any unnecessary application services that are available are considered to be a failure in setting the filter rules. Figure 17 shows the static network topology of Scenario 1.

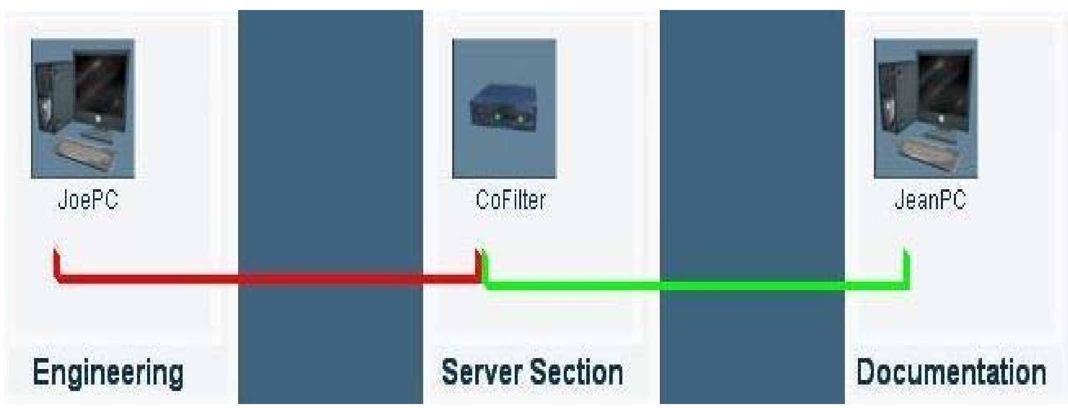


Figure 17 Scenario 1 Network Topology

2. Scenario 1: Test Case 1

All application service requests are denied FROM and/or TO LAN 1 except for Database. Database application service requests are not allowed to LAN 1 and they can be sent from LAN 1 as shown in Table 35.

When this objective is achieved, a ticker message shall display *“Great! You have successfully protected the Project Firebird using the filtering rule”* and the player has successfully completed Scenario 1.

	Network	LAN 1		LAN 2	
	Application Service	**To**	**From**	**To**	**From**
1	Web Server	[X]	[X]	[D]	[D]
2	eMail Server	[X]	[X]	[D]	[D]
3	Telnet	[X]	[X]	[D]	[D]
4	FTP	[X]	[X]	[D]	[D]
5	SSH	[X]	[X]	[D]	[D]
6	Database	[X]	[ ]	[ ]	[D]
7	Defense Rat	[X]	[X]	[D]	[D]
8	Defense 4T	[X]	[X]	[D]	[D]
9	VPN Gateway	[X]	[X]	[D]	[D]
10	Reporting	[X]	[X]	[D]	[D]
11	Management	[X]	[X]	[D]	[D]
12	Internal IP Addresses	[X]	[X]	[D]	[D]

Table 35 Scenario 1 Test Case 1

3. Scenario 1: Test Case 2

In this test case, the filtering rules can be configured on LAN 2 of the firewall. On LAN 2, all application services except the Database application service requests should not be allowed from LAN 2, and the Database application service request is allowed to LAN 1 as shown in Table 36.

Similarly, as in Test Case 1, a ticker message would display *"Great! You have successfully protected the Project Firebird using the filtering rule"* when the objective is met.

	Network	LAN 1		LAN 2	
	Application Service	To	From	To	From
1	Web Server	[D]	[D]	[X]	[X]
2	eMail Server	[D]	[D]	[X]	[X]
3	Telnet	[D]	[D]	[X]	[X]
4	FTP	[D]	[D]	[X]	[X]
5	SSH	[D]	[D]	[X]	[X]
6	Database	[D]	[ ]	[ ]	[X]
7	Defense Rat	[D]	[D]	[X]	[X]
8	Defense 4T	[D]	[D]	[X]	[X]
9	VPN Gateway	[D]	[D]	[X]	[X]
10	Reporting	[D]	[D]	[X]	[X]
11	Management	[D]	[D]	[X]	[X]
12	Internal IP Addresses	[D]	[D]	[X]	[X]

Table 36 Scenario 1 Test Case 2

4. Scenario 1: Test Case 3

Test Case 3 provides an exhaustive test on the wrong setting of Database application service on LAN 1 and LAN 2 of the firewall interface. It is assumed that all application services except for the Database are configured according to either Table 35 or Table 36. Table 37 shows the possible feedback messages when a mistake is made on the filtering rules of the Database application service:

	Network	LAN 1		LAN 2		
	Application Service	To	From	To	From	Message (See Legend)
1	Database	[ ]	[ ]	[ ]	[ ]	T2

	Network	LAN 1		LAN 2		
	Application Service	**To**	**From**	**To**	**From**	**Message (See Legend)**
2	Database	[ ]	[ ]	[X]	[ ]	T2 and T3
3	Database	[ ]	[ ]	[X]	[X]	T3
4	Database	[ ]	[X]	[ ]	[ ]	T2 and T3
5	Database	[ ]	[X]	[ ]	[X]	T3
6	Database	[ ]	[X]	[X]	[ ]	T2 and T3
7	Database	[ ]	[X]	[X]	[X]	T3
8	Database	[X]	[ ]	[X]	[ ]	T3
9	Database	[X]	[ ]	[X]	[X]	T3
10	Database	[X]	[X]	[ ]	[ ]	T3
11	Database	[X]	[X]	[ ]	[X]	T3
12	Database	[X]	[X]	[X]	[ ]	T3
13	Database	[X]	[X]	[X]	[X]	T3

Table 37 Scenario 1 Test Case 3

C. SCENARIO 2 TESTING

In Scenario 2, players are required to complete three phases in order to win the game. A network topology, as shown in Figure 18, is in place when Scenario 2 is launched. The players are required to change the network topologies and set the filtering rules to meet the objectives of the game. Table 38 is the legend used for the test cases in Scenario 2.

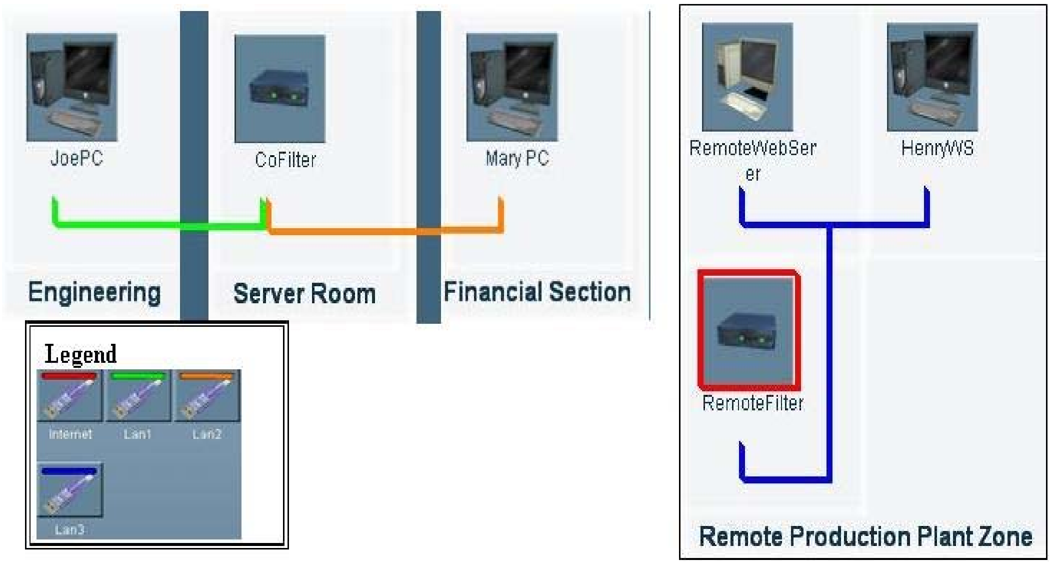


Figure 18 Scenario 2 Network Topology

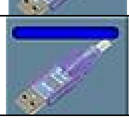
Symbol	Description
[ ]	Permit
[X]	Deny
[D]	Don’t Care
T4	Jean Speak Trigger: *“Why can’t I access the Internet?”*
T5	Jean Speak Trigger: *“Is there a problem with the Internet?”*
T6	Ticker message: *“Firewall log review shows that there are internal IP spoofing incidents.”*
T7	Mary Speak Trigger: *“Why is my system slow?”*
T8	Joe Speak Trigger: *“Why is my system so slow? Why am I getting these funny messages?”*
	Internet
	LAN 1
	LAN 2
	LAN 3

Table 38 Scenario 2 Legend

1. Overview of Scenario 2

In this scenario, there are three assets, namely ‘Remote WebAsset’, ‘Project Firebird’ and ‘Account Book’, which reside on RemoteWebServer, JoePC and MaryPC

respectively. Remote WebAsset can be accessed using the Web Server. Both Project Firebird and Account Book can be accessed through the Database service.

2. Phase 0

In this phase, the objective is to provide the Internet connection such that Joe and Mary are able to access the Remote WebAsset which resides on the remote site. This objective can be achieved by adding a network. However, there are two network topologies and several filtering rule variations that can fulfill this phase. Any one of the two network topology solutions should allow the players to proceed to Phase 1.

a. Phase 0: Test Case 4

Test Case 4 is to verify that when an Internet connection is established, as shown in Figure 19, and correct filtering rules are instituted for the Web Server application of Firewall 1 as shown in Table 39, the game should proceed to Phase 1. *"Great. Joe and Mary are happy to have Internet access again. See Next Objective"* would pop up to inform the players of the successful completion of Phase 0. The status of the other application services in the firewall has no impact on the successful completion of Phase 0.

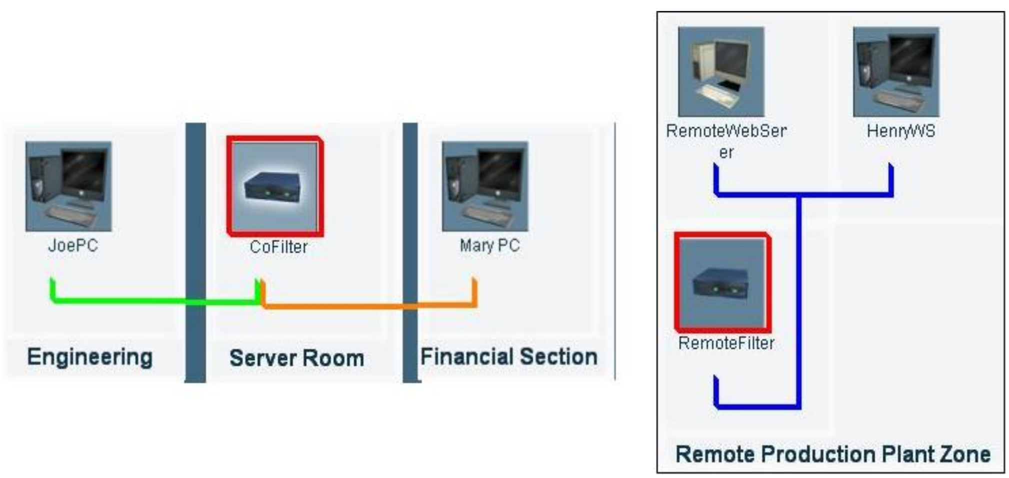


Figure 19 Scenario 2 Perfect Internet Connection

	Network	Internet		LAN 1		LAN 2	
	Application Service	**To**	**From**	**To**	**From**	**To**	**From**
1	Web Server	[ ]	[D]	[D]	[ ]	[D]	[ ]

Table 39 Scenario 2 Test Case 4

b. Phase 0: Test Case 5

This test case is used to verify that when the filtering rules are on but the filters are not properly configured, the game will deny the players from proceeding to Phase 1. It is assumed that the network topology in Figure 19 is adopted. Any deviation of the filtering rules as shown in Table 39 would deny the players from proceeding to Phase 1. Table 40 shows a list of possible feedback when the filtering rules on the Web Server are incorrectly setup.

	Network	**LAN 3 / Internet**		**LAN 1**		**LAN 2**		
	Application Service	**To**	**From**	**To**	**From**	**To**	**From**	**Message (See Legend)**
1	Web Server	[ ]	[D]	[D]	[ ]	[D]	[X]	T4
2	Web Server	[ ]	[D]	[D]	[X]	[D]	[ ]	T5
3	Web Server	[ ]	[D]	[D]	[X]	[D]	[X]	T4 and T5
4	Web Server	[X]	[D]	[D]	[ ]	[D]	[ ]	T4 and T5
5	Web Server	[X]	[D]	[D]	[ ]	[D]	[X]	T4 and T5
6	Web Server	[X]	[D]	[D]	[X]	[D]	[ ]	T4 and T5
7	Web Server	[X]	[D]	[D]	[X]	[D]	[X]	T4 and T5

Table 40 Test Case 5

3. Phase 1

The objective of Phase 1 is to deny any traffic from the Internet that is trying to spoof the organization’s internal IP network. At the same time, Mary and Joe need to continue to access the Internet.

a. Phase 1: Test Case 6

This test case is to verify that when the filter is configured to deny any traffic from the Internet trying to spoof the internal network IP address, it will allow the game to advance to Phase 2. It is assumed that the filtering rule is configured in such a manner that Mary and Joe are able to access the Internet as shown in Table 39. The

player will be allowed to proceed to Phase 2 when either of the options in Table 41 is used. A pop-up message of "*You have successfully prevented anyone from the Internet to spoof your internal network*" will appear.

	Network	Internet/LAN 3		LAN 1		LAN 2	
	Application Service	**To**	**Fro m**	**To**	**From**	**To**	**From**
1	Internal IP Address	[ ]	[D]	[X]	[ ]	[X]	[ ]
2	Internal IP Address	[ ]	[X]	[D]	[ ]	[D]	[ ]

Table 41 Test Case 6

b. Phase 1: Test Case 7

Test Case 7 is used to verify that when the filter rules on Internal IP address are incorrectly set, they will not permit the players to proceed to Phase 2. Table 42 is a list of possible mistakes that players can make in the filtering rules. Different mistakes for Internal IP address filtering may result in different feedback.

	Network	LAN 3 / Internet		LAN 1		LAN 2		
	Application Service	**To**	**From**	**To**	**From**	**To**	**From**	**Feedback**
1	Internal IP Address	[D]	[ ]	[ ]	[D]	[ ]	[D]	T6
2	Internal IP Address	[D]	[ ]	[X]	[D]	[ ]	[D]	T7
3	Internal IP Address	[D]	[ ]	[ ]	[D]	[X]	[D]	T8

Table 42 Test Case 7

4. Phase 2

In the final phase of Scenario 2, the requirements for the filtering rules are more stringent. The players have to continue to fulfill the two objectives mentioned earlier in this scenario and, in addition, have to ensure that unnecessary application services that are not required are denied from the Internet as well as from the internal network. This is to tighten the network security and keep the network from being exploited by the public as well as employees. At the same time, Mary is required to access the asset Project Firebird, which resides on Joe's computer, using the Database application service.

a. Phase 2: Test Case 8

Test Case 8 is used to verify that the filtering rule as shown in Table 43 will allow the players to win the game of Scenario 2. A win trigger will display the message: *"You have successfully completed Scenario 2. Go to Scenario 3 for more challenges."*

	Network	LAN 3/ Internet		LAN 1		LAN 2	
	Application Service	**To**	**Fro m**	**To**	**From**	**To**	**From**
1	Web Server	[ ]	[X]	[X]	[ ]	[X]	[ ]
2	eMail Server	[X]	[X]	[X]	[X]	[X]	[X]
3	Telnet	[X]	[X]	[X]	[X]	[X]	[X]
4	FTP	[X]	[X]	[X]	[X]	[X]	[X]
5	SSH	[X]	[X]	[X]	[X]	[X]	[X]
6	Database	[X]	[X]	[ ]	[X]	[X]	[ ]
7	Defense Rat	[X]	[X]	[X]	[X]	[X]	[X]
8	Defense 4T	[X]	[X]	[X]	[X]	[X]	[X]
9	VPN Gateway	[X]	[X]	[X]	[X]	[X]	[X]
10	Reporting	[X]	[X]	[X]	[X]	[X]	[X]
11	Management	[X]	[X]	[X]	[X]	[X]	[X]
12	Internal IP Addresses	[X]	[X]	[X]	[X]	[X]	[X]

Table 43 Test Case 8

b. Phase 2: Test Case 9

All application services in the filtering rules are denied as shown in Table 44. In Test Case 9, several messages are displayed to inform the players that they are required to setup the filtering rules for the Web Server and the Database application services. *"Joe and Mary still need Internet access"* and *"Filter Rules between LAN 1 and LAN 2 are incorrect"* are the two warning messages displayed to the players.

	Network	LAN 3/ Internet		LAN 1		LAN 2	
	Application Service	**To**	**Fro m**	**To**	**From**	**To**	**From**
1	Web Server	[X]	[X]	[X]	[X]	[X]	[X]
2	eMail Server	[X]	[X]	[X]	[X]	[X]	[X]
3	Telnet	[X]	[X]	[X]	[X]	[X]	[X]
4	FTP	[X]	[X]	[X]	[X]	[X]	[X]
5	SSH	[X]	[X]	[X]	[X]	[X]	[X]
6	Database	[X]	[X]	[X]	[X]	[X]	[X]
7	Defense Rat	[X]	[X]	[X]	[X]	[X]	[X]
8	Defense 4T	[X]	[X]	[X]	[X]	[X]	[X]
9	VPN Gateway	[X]	[X]	[X]	[X]	[X]	[X]
10	Reporting	[X]	[X]	[X]	[X]	[X]	[X]
11	Internal IP Addresses	[X]	[X]	[X]	[X]	[X]	[X]
12	Management	[X]	[X]	[X]	[X]	[X]	[X]

Table 44 Test Case 9

c. Phase 2: Test Case 10

Test Case 11 is used to verify that the Web Server can be exploited between LAN 1 and LAN 2. A feedback message would display *"Filter Rules between LAN 1 and LAN 2 are incorrect"* when the filter rules on the Web Server and Database are set according to Table 45.

	Network	LAN 3/ Internet		LAN 1		LAN 2	
	Application Service	**To**	**Fro m**	**To**	**From**	**To**	**From**
1	Web Server	[ ]	[X]	[ ]	[ ]	[ ]	[ ]

	Network	LAN 3/ Internet		LAN 1		LAN 2	
	Application Service	**To**	**Fro m**	**To**	**From**	**To**	**From**
2	eMail Server	[X]	[X]	[X]	[X]	[X]	[X]
3	Telnet	[X]	[X]	[X]	[X]	[X]	[X]
4	FTP	[X]	[X]	[X]	[X]	[X]	[X]
5	SSH	[X]	[X]	[X]	[X]	[X]	[X]
6	Database	[X]	[X]	[ ]	[X]	[X]	[ ]
7	Defense Rat	[X]	[X]	[X]	[X]	[X]	[X]
8	Defense 4T	[X]	[X]	[X]	[X]	[X]	[X]
9	VPN Gateway	[X]	[X]	[X]	[X]	[X]	[X]
10	Reporting	[X]	[X]	[X]	[X]	[X]	[X]
11	Internal IP Addresses	[X]	[X]	[X]	[X]	[X]	[X]
12	Management	[X]	[X]	[X]	[X]	[X]	[X]

Table 45 Test Case 10

D. SCENARIO 3 TESTING

This scenario is comprised of three phases. The players have to decide which network topologies are suitable to manage the access control for the public and private servers. Eventually, the requirement in Phase 2 requires the player to set up two filtering devices in order to effectively protect the organization’s valuable assets. Scenario 3 starts with a network topology as shown in Figure 20. Table 46 shows the legend used in Scenario 3.

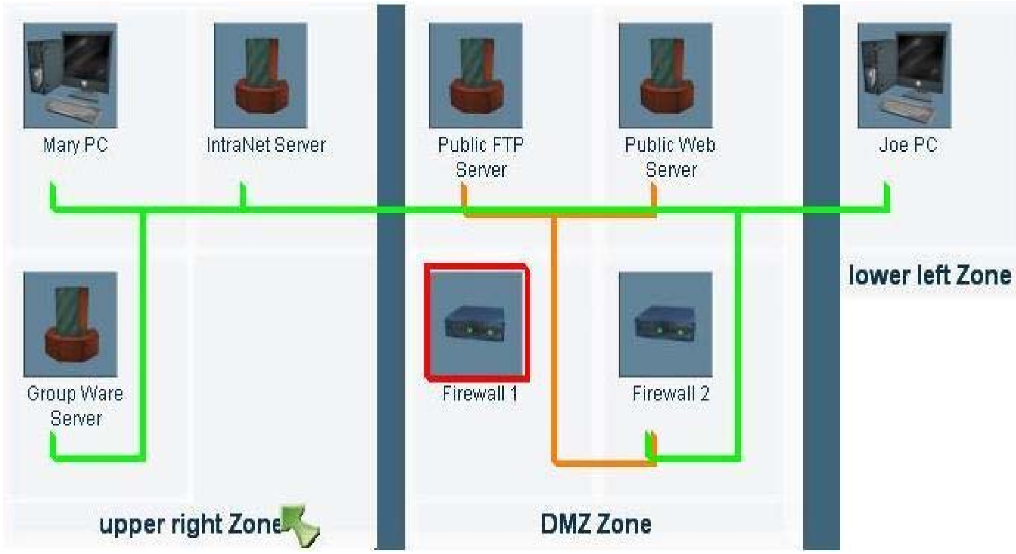


Figure 20 Scenario 3 Initial Network Topology

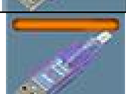
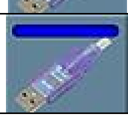
Symbol	Description
[ ]	Permit
[X]	Deny
[D]	Don’t Care
T9	Ticker Trigger: *“Employees can’t access Public Servers”*
T10	Ticker Trigger: *“Employees can’t access Public FTP Server”*
T11	Ticker Trigger: *“Employees can’t access Public Web Server”*
T12	Ticker Trigger: *“Both Joe and Mary are upset, they can't access Internet.”*
	Internet
	LAN 1
	LAN 2
	LAN 3

Table 46 Scenario 3 Legend

1. Scenario 3 Overview

The seven assets, namely ‘Firebird’, ‘Financial Account’, ‘Private IntraNet Data’, ‘Private Group Ware Data’, ‘Public FTP Data’, ‘Public Web Data’ and ‘Remote WebAsset’ reside in the machine of ‘Joe PC’, ‘Mary PC’, ‘IntraNet Server’, ‘Group Ware

Server', Public FTP Server', 'Public Web Server' and 'Remote Web Server', respectively. Private IntraNet Data and Private Group Ware Data can be accessed by employees using Database and Management application services. Public FTP Data and Public Web Data can be accessed using FTP and Web Server applications by employees and the public. The 'Remote WebAsset' needs to be accessed by the employee using the Web Server.

2. Phase 0

In Phase 0, both Joe and Mary need to access public servers and the Internet. The players can have two options to fulfill the objective of Phase 0 in Test Case 1 and Test Case 2. These are described below.

a. Phase 0: Test Case 11

In Phase 0, either one of the network topologies as shown in Figure 21 or Figure 22 can achieve the objective for Phase 0. The filter rules as shown in Table 47 and Table 48 applied on Firewall 1 and Firewall 2, respectively, would allow the player to proceed to Phase 1. A message pops up to inform the players that they have successfully completed Phase 0. The message is *"Well Done! Joe and Mary are able to access the Internet and Public Servers. See the Next Objective."*

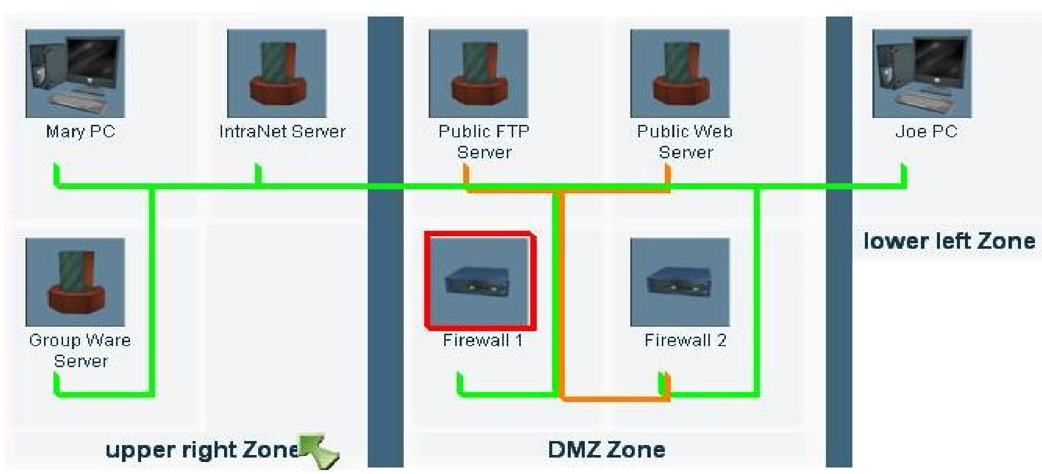


Figure 21 Using LAN 1

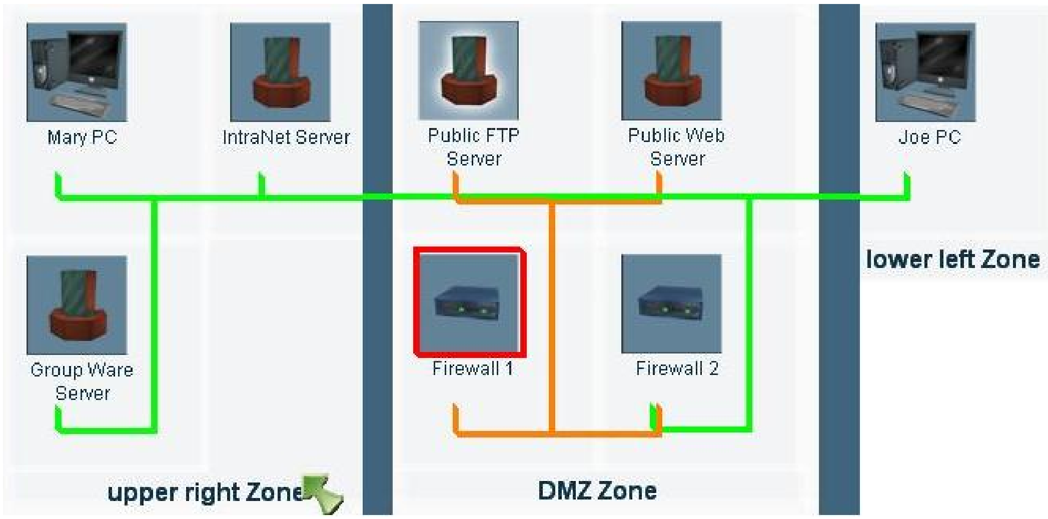


Figure 22 Using LAN 2 to create DMZ

	Network	Internet		LAN 1 / LAN 2	
	Application Service	**To**	**Fro m**	**To**	**From**
1	Web Server	[ ]	[D]	[D]	[ ]
2	FTP	[D]	[D]	[D]	[D]

Table 47 Test Case 11a on Firewall 1

	Network	LAN 1		LAN 2	
	Application Service	**To**	**From**	**To**	**From**
1	Web Server	[D]	[ ]	[ ]	[D]
2	FTP	[D]	[ ]	[ ]	[D]

Table 48 Test Case 11b on Firewall 2

b. Phase 0: Test Case 12

With the network topology as shown in Figure 21 or Figure 22 and the setting of filtering rules as shown in Table 47 for Firewall 1, and Table 49 for Firewall 2, the players are informed that "*Employees can't access the public servers*" and/or "*Both Joe and Mary are upset, they can't access the Internet.*"

	Network	LAN 1		LAN 2	
	Application Service	To	From	To	From
1	Web Server	[D]	[X]	[D]	[D]
2	FTP	[D]	[X]	[D]	[D]

Table 49 Test Case 12 on Firewall 2

c. Phase 0: Test Case 13

Using the same setup as Scenario 3 Test Case 12, except for the filtering rules in Firewall 2, the players receive feedback that indicates the reasons for not being able to proceed to Phase 1. The test case conditions are as shown in Table 50 and Table 51.

	Network	LAN 1		LAN 2		
	Application Service	To	From	To	From	Message (See Legend)
1	Web Server	[D]	[ ]	[D]	[D]	
2	FTP	[D]	[X]	[D]	[D]	T10

Table 50 Test Case 13a on Firewall 2

	Network	LAN 1		LAN 2		
	Application Service	To	From	To	From	Message (See Legend)
1	Web Server	[D]	[X]	[D]	[D]	T11, T12
2	FTP	[D]	[ ]	[ ]	[D]	

Table 51 Test Case 13b on Firewall 2

3. Phase 1

The objective for Phase 1 is to fulfill the following requirements:

- Allow the public and employees to access the public servers.
- Allow Joe and Mary to have Internet access.
- Prevent IP spoofing from the Internet.
- Deny all unnecessary application services between the Internet and LAN 1.

The assumption of this test case in this phase is that the filtering rules on all the application services of Firewall 2 are not blocked.

a. Phase 1: Test Case 14

The player is allowed to advance to Phase 2 when the filtering rules on Firewall 1 are configured as shown in Table 52.

	Network	**Internet**		**LAN 1 / LAN 2**	
	Application Service	**To**	**Fro m**	**To**	**From**
1	Web Server	[ ]	[ ]	[ ]	[ ]
2	eMail Server	[X]	[X]	[D]	[D]
3	Telnet	[X]	[X]	[D]	[D]
4	FTP	[X]	[ ]	[ ]	[D]
5	SSH	[X]	[X]	[D]	[D]
6	Database	[X]	[X]	[D]	[D]
7	Defense Rat	[X]	[X]	[D]	[D]
8	Defense 4T	[X]	[X]	[D]	[D]
9	VPN Gateway	[X]	[X]	[D]	[D]
10	Reporting	[X]	[X]	[D]	[D]
11	Management	[X]	[X]	[D]	[D]
12	Internal IP Addresses	[X]	[X]	[D]	[D]

Table 52 Test Case 14 on Firewall 1

b. Phase 1: Test Case 15

This test case is to verify that there are unnecessary application services available to insiders. For example, in Table 53, the ‘eMail Server’ application can be exploited by employees on LAN 1 to the Internet. A ticker message would appear stating that “*Joe is exporting other application services to the Internet.*”

	Network	**Internet**		**LAN 1 / LAN 2**	
	Application Service	**To**	**Fro m**	**To**	**From**
1	Web Server	[ ]	[ ]	[ ]	[ ]
2	eMail Server	[ ]	[X]	[D]	[ ]
3	Telnet	[D]	[X]	[D]	[D]
4	FTP	[D]	[ ]	[ ]	[D]
5	SSH	[D]	[X]	[D]	[D]
6	Database	[D]	[X]	[D]	[D]
7	Defense Rat	[D]	[X]	[D]	[D]
8	Defense 4T	[D]	[X]	[D]	[D]
9	VPN Gateway	[D]	[X]	[D]	[D]
10	Reporting	[D]	[X]	[D]	[D]
11	Management	[D]	[X]	[D]	[D]
12	Internal IP Addresses	[X]	[X]	[D]	[D]

Table 53 Test Case 15 on Firewall 1

c. Phase 1: Test Case 16

The purpose of this test case is to verify that there are too many application services available that might be exploited by people from the Internet. For example, in Table 54, public users from the Internet can exploit the ‘eMail Server’ application to access the organization network. “*Are there too many application services*

available to the public?" would appear as a ticker message to warn the players of such danger.

	Network	Internet		LAN 1 / LAN 2	
	Application Service	**To**	**Fro m**	**To**	**From**
1	Web Server	[ ]	[ ]	[ ]	[ ]
2	eMail Server	[X]	[ ]	[ ]	[D]
3	Telnet	[X]	[D]	[D]	[D]
4	FTP	[X]	[ ]	[ ]	[D]
5	SSH	[X]	[D]	[D]	[D]
6	Database	[X]	[D]	[D]	[D]
7	Defense Rat	[X]	[D]	[D]	[D]
8	Defense 4T	[X]	[D]	[D]	[D]
9	VPN Gateway	[X]	[D]	[D]	[D]
10	Reporting	[X]	[D]	[D]	[D]
11	Management	[X]	[D]	[D]	[D]
12	Internal IP Addresses	[X]	[X]	[D]	[D]

Table 54 Test Case 16 on Firewall 1

d. Phase 1: Test Case 17

Test Case 17 is used to verify that the players have considered denying any IP spoofing coming from the Internet. When the players fail to deny any traffic using an internal IP address as shown in Table 55, *"Is your network vulnerable to internal IP Spoofing?"* appears as a ticker message.

	Network	Internet		LAN 1 / LAN 2	
	Application Service	**To**	**Fro m**	**To**	**From**
1	Web Server	[ ]	[ ]	[ ]	[ ]

	Network	Internet		LAN 1 / LAN 2	
	Application Service	**To**	**Fro m**	**To**	**From**
2	eMail Server	[X]	[X]	[D]	[D]
3	Telnet	[X]	[X]	[D]	[D]
4	FTP	[X]	[ ]	[ ]	[D]
5	SSH	[X]	[X]	[D]	[D]
6	Database	[X]	[X]	[D]	[D]
7	Defense Rat	[X]	[X]	[D]	[D]
8	Defense 4T	[X]	[X]	[D]	[D]
9	VPN Gateway	[X]	[X]	[D]	[D]
10	Reporting	[X]	[X]	[D]	[D]
11	Management	[X]	[X]	[D]	[D]
12	Internal IP Addresses	[X]	[ ]	[ ]	[D]

Table 55 Test Case 17

4. Phase 2

In Phase 2, the objectives are:

- Joe and Mary need to have Internet access.
- Need to prevent IP Spoofing from the Internet.
- The Public and employees can access the public servers (Public Web Server and Public FTP Server).
- The Public must be denied access to the private servers (IntraNet Server and GroupWare Server).
- All unnecessary application services must be denied.

Using the network topology as shown in Figure 21, it is unlikely the player can win the game. Players have to use the network topology as shown in Figure 22. In this

way, the players can control the availability of application services to and from the Internet and the private network. It is essential to use both Firewall 1 and Firewall 2.

a. Phase 2: Test Case 18

This phase verifies that the players need to setup the correct network topology and filtering rules on both firewalls before they can successfully complete the Scenario 3. Using Figure 22 as the network topology, Table 52 for the Firewall 1 configuration and Table 56 for Firewall 2, the players will win the game.

	Network	**LAN 1**		**LAN 2**	
	Application Service	**To**	**From**	**To**	**From**
1	Web Server	[X]	[ ]	[ ]	[D]
2	eMail Server	[X]	[X]	[D]	[D]
3	Telnet	[X]	[X]	[D]	[D]
4	FTP	[X]	[ ]	[ ]	[D]
5	SSH	[X]	[X]	[D]	[D]
6	Database	[X]	[X]	[D]	[D]
7	Defense Rat	[X]	[X]	[D]	[D]
8	Defense 4T	[X]	[X]	[D]	[D]
9	VPN Gateway	[X]	[X]	[D]	[D]
10	Reporting	[X]	[X]	[D]	[D]
11	Management	[X]	[X]	[D]	[D]
12	Internal IP Addresses	[X]	[X]	[D]	[D]

Table 56 Test Case 18 on Firewall 2

b. Phase 2: Test Case 19

Using Figure 22 as the network topology, Table 52 on Firewall 1 and Table 57 on Firewall 2, the players are warned that *"Joe and Mary cannot access the Public Server"* and *"Malicious application services have sneaked onto the private*

servers and have destroyed information. Information on the servers has to be reinstalled."

	Network	LAN 1		LAN 2	
	Application Service	**To**	**From**	**To**	**From**
1	Web Server	[X]	[X]	[D]	[D]
2	eMail Server	[X]	[X]	[D]	[D]
3	Telnet	[X]	[X]	[D]	[D]
4	FTP	[X]	[X]	[D]	[D]
5	SSH	[X]	[X]	[D]	[D]
6	Database	[X]	[X]	[D]	[D]
7	Defense Rat	[X]	[X]	[D]	[D]
8	Defense 4T	[X]	[X]	[D]	[D]
9	VPN Gateway	[X]	[X]	[D]	[D]
10	Reporting	[X]	[X]	[D]	[D]
11	Management	[X]	[X]	[D]	[D]
12	Internal IP Addresses	[X]	[X]	[D]	[D]

Table 57 Test Case 19 on Firewall 2

c. Phase 2: Test Case 20

The purpose of this phase is to verify that the FTP and Web Server application services have been denied in the correct network topology of Figure 22.*"Joe and Mary cannot access Public Server"* and *"Joe and Mary can't access the Internet"* are the two ticker messages that appear when the filtering rules are set according to Table 58.

	Network	LAN 1		LAN 2	
	Application Service	To	From	To	From
1	Web Server	[X]	[X]	[ ]	[D]
2	eMail Server	[X]	[X]	[D]	[D]
3	Telnet	[X]	[X]	[D]	[D]
4	FTP	[X]	[X]	[ ]	[D]
5	SSH	[X]	[X]	[D]	[D]
6	Database	[X]	[X]	[D]	[D]
7	Defense Rat	[X]	[X]	[D]	[D]
8	Defense 4T	[X]	[X]	[D]	[D]
9	VPN Gateway	[X]	[X]	[D]	[D]
10	Reporting	[X]	[X]	[D]	[D]
11	Management	[X]	[X]	[D]	[D]
12	Internal IP Addresses	[X]	[X]	[D]	[D]

Table 58 Test Case 20 on Firewall 2

d. Phase 2: Test Case 21

In this test case, Table 59 indicates that the FTP application service has been denied. *"Joe and Mary need access to the Public FTP Server"* are displayed to the player.

	Network	LAN 1		LAN 2	
	Application Service	To	From	To	From
1	Web Server	[X]	[ ]	[ ]	[D]
2	eMail Server	[X]	[X]	[D]	[D]

	Network	LAN 1		LAN 2	
	Application Service	**To**	**From**	**To**	**From**
3	Telnet	[X]	[X]	[D]	[D]
4	FTP	[X]	[X]	[ ]	[D]
5	SSH	[X]	[X]	[D]	[D]
6	Database	[X]	[X]	[D]	[D]
7	Defense Rat	[X]	[X]	[D]	[D]
8	Defense 4T	[X]	[X]	[D]	[D]
9	VPN Gateway	[X]	[X]	[D]	[D]
10	Reporting	[X]	[X]	[D]	[D]
11	Management	[X]	[X]	[D]	[D]
12	Internal IP Addresses	[X]	[X]	[D]	[D]

Table 59 Test Case 21 on Firewall 2

E. TEST RESULTS

The test cases for the three scenarios were conducted. The following tables provide a summary of the actual results obtained for each scenario.

1. Scenario 1 Test Results

For each test case, the results for running Scenario 1 are tabulated as shown in Table 60. From the results, it can be seen that the conditions and triggers mechanism of the game are implemented correctly and meet the design expectations.

Test Case No.	Expectations Met
1	Pass / ~~Fail~~
2	Pass / ~~Fail~~
3	Pass / ~~Fail~~

Table 60 Result of Test Case 1 to 3

2. Scenario 2 Test Results

The test for Scenario 2 is similar to those for Scenario 1. The outputs of the results are recorded in Table 61. The results show that the design expectations were met.

Test Case No.	Expectations Met
4	Pass / ~~Fail~~
5	Pass / ~~Fail~~
6	Pass / ~~Fail~~
7	Pass / ~~Fail~~
8	Pass / ~~Fail~~
9	Pass / ~~Fail~~
10	Pass / ~~Fail~~

Table 61 Result of Test Case 4 to 10

3. Scenario 3 Test Results

The test for Scenario 3 is similar to that for Scenario 1 and 2. The results are recorded in Table 62 and the results show that design expectations were met.

Test Case No.	Expectations Met
11	Pass / ~~Fail~~
12	Pass / ~~Fail~~
13	Pass / ~~Fail~~
14	Pass / ~~Fail~~
15	Pass / ~~Fail~~
16	Pass / ~~Fail~~
17	Pass / ~~Fail~~
18	Pass / ~~Fail~~
19	Pass / ~~Fail~~

Test Case No.	Expectations Met
20	Pass / ~~Fail~~
21	Pass / ~~Fail~~

Table 62 Result of Test Case 11 to 21

F. LIMITATION AND BUGS

There are some limitations in what the SDT can support in the development of scenarios that are meant for educational purposes. This section shall highlight some of the limitations encountered and how they were overcome. During scenario development, several bugs were encountered.

1. Game Attack Engine

As highlighted in Chapter III, the main focus of the three scenarios was to provide continuous feedback to the players of their progress in fulfilling the users' goals. In the initial phase of scenario development, the game engine attacks were used but the feedback from the engine attacks were found to be unpredictable. This behavior made it hard for the game developers to generate the correct positive and negative feedback for the players. Thus, the game engine attacks were not used in the three scenarios.

2. Error in AssetToNetworkByFilterType Specification

Table 63 shows the technical specification of *AssetToNetworkByFilterType* condition class described in Scenarios Format Template Version 15g. In this document, the mode field value in the "Description" column was incorrectly documented. The functionality does not behave according to specification.

AssetToNetworkByFilterType	Whether a named asset can be reached via a given network through a software filter	
Parameter	Name (Displayed in tool)	Description
ConditionText	Asset	Asset name
SecondConditionText	Network	Network name
ThirdConditionText	SoftwareType	Software Type
Parameter	Mode	0 = both, 1 = in, 2= out

Table 63 Incorrect Specification [From Ref. [18]]

An experiment was carried out to test the functionality of the *AssetToNetworkByFilterType*. Using the specification as the standard, the experiment showed that the description on the specification does not match the experienced results. The experiment when the mode = 1 (IN) showed that it has the same result as the description of the specification. When the value of *AssetToNetworkByFilterType* condition class mode is set to zero (mode = 0 (both)), the functionality of the *AssetToNetworkByFilterType* behaved as if the mode is set to 2 (mode =2 (out)). Likewise, when the mode is set to two, the functionality of *AssetToNetworkByFilterType* behaved as if it is set to zero.

To avoid changing the CyberCIEGE source, it is assumed that the specification has an error, therefore, by changing the mode = 0 (OUT) and mode = 2 (BOTH), the functionality and specification issues are resolved.

3. Filter Anomalies Resulting from More Than Two Networks

There is a bug on the attack engine that affects the development of the filter game. Unexpected behavior occurs when more than two networks are connected to a filter. The filtering rule does not work correctly. The behavior is described as follows:

In a simple network topology, as shown in Figure 23, an asset, ‘Info J’, resides on Joe PC and another asset, ‘Info H’, resides on Hacker PC. The filtering rules on the filter do not block any application services, so Info H and Info J can be accessed from LAN 1 and LAN 2 respectively using the Web Server application service. The filter rules are setup such that Info H can be accessed from LAN 1 and Info J cannot be accessed from LAN 2. The functionality of the game is working according to the specification. With the same configuration of the filter rules, a new network or the Internet is connected to the filter device as shown in Figure 24. With that connection, there should not be any changes to access to the assets between LAN 1 and LAN 2. However, that was never the case. With a new network or the Internet connection to the existing network, Info J can be accessed on LAN 2. This problem was reported. A software bug was found in the attack engine and it has been resolved.

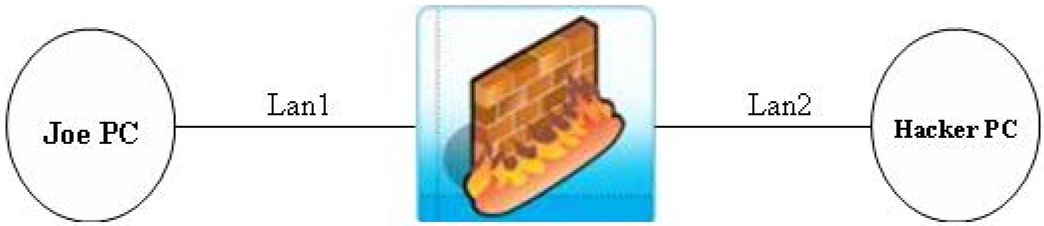


Figure 23 Simple Network

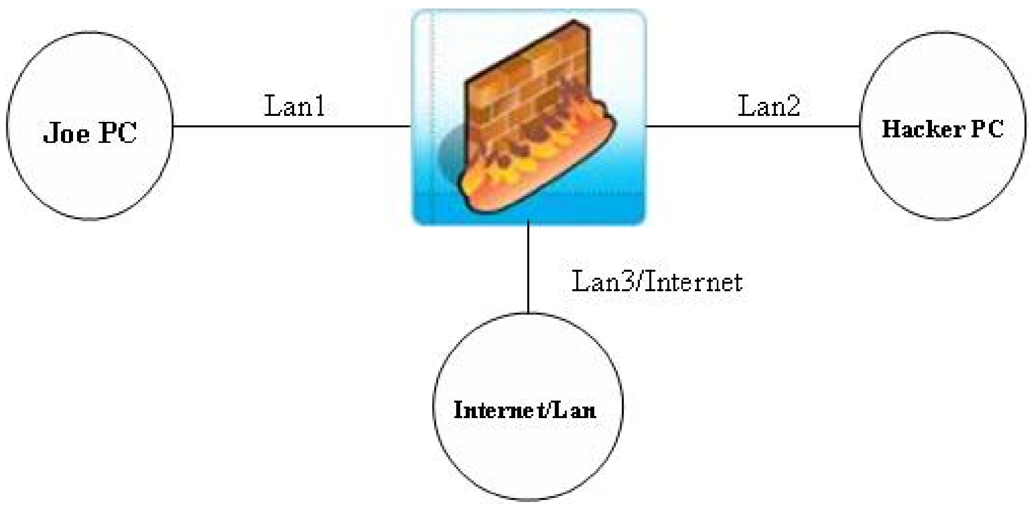


Figure 24 Introduction of a new network

4. Game Crash from Disconnecting Networks

During the development of the game, another software bug was discovered. This bug will cause the game to be terminated when a network is disconnected at the computer or workstation component as shown in Figure 25.

For example, when the ’JoePC’ or ’HackerPC’ component is selected and a command is issued to remove the network, the game is terminated prematurely. On the other hand, if ’CoFilter’ is selected and a command is issued to remove the network, play can continue as expected. This problem was reported and resolved. A bug was found in the game engine.

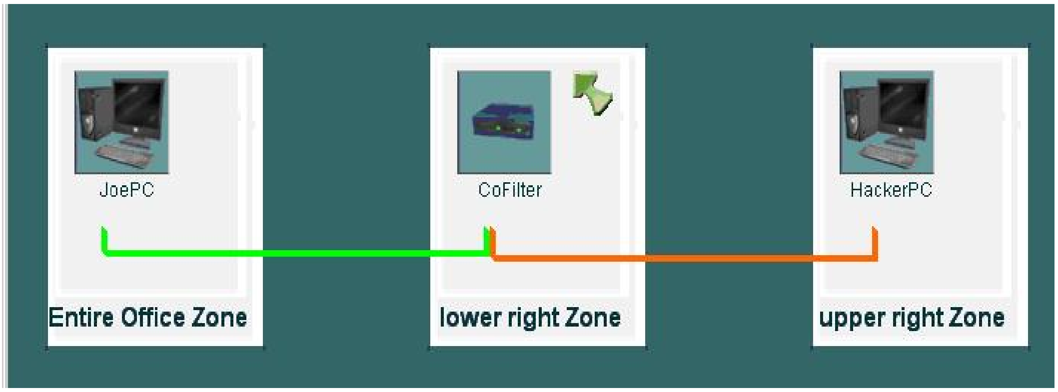


Figure 25 Simple Network 2

G. SUMMARY

This chapter described the test strategy and important test cases which indicated the scope as well as the expected and actual results.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION AND RECOMMENDATION

A. CONCLUSION

The purpose of developing this thesis is to contribute to the Naval Postgraduate School's ongoing CyberCIEGE research, which supports the development of teaching tools in the area of information assurance (IA).

The three scenarios developed by this research reinforce firewall concepts such as "What is a firewall?", "Why would anybody need one?", and "What can it protect?". The differences between a real firewall and the CyberCIEGE firewall, and whether a CyberCIEGE firewall can be used as effective teaching tools are addressed in this research. From the experiments conducted to evaluate CyberCIEGE filtering, it is concluded that CyberCIEGE uses only packet filtering techniques. It uses a simplified rule set as an aid to understanding filtering. The protection that firewalls provide can be no better than the policies they are configured to implement. The scenarios were developed to highlight that configuration is a crucial task when using firewalls as a protection mechanism. A filtering campaign, comprised of three scenarios, was developed to demonstrate that CyberCIEGE can provide a 'simulated environment' on filtering in which various forms of learning can take place. The scenario activities help the player of the game to develop knowledge and skills through its contents while playing the game. Through this game, knowledge related to firewall deployment can be imparted and skills can be developed primarily through planning and deployment strategies.

B. RECOMMENDATIONS

In the development and testing phase of the CyberCIEGE game, ideas for improving the tool were identified as summarized below.

1. IP Address and Port Number

As discussed in Chapter II, a firewall usually inspects the header information of each incoming and outgoing TCP/IP packet, specifically in the source and destination IP addresses and port numbers. In the current version of CyberCIEGE, the filtering component does not support the packet filtering based on IP addresses and port numbers. If CyberCIEGE allowed filtering rules to deny traffic associated with IP addresses and port numbers, the filtering element of CyberCIEGE would be more realistic. To achieve

this, CyberCIEGE would have to be adapted to manage IP addresses for components and sub-networks, and would need to make these visible to players in a meaningful manner.

2. Data Logging

CyberCIEGE has built-in data logging capability that provides plain text feedback about a player's progress in the game. This data log information can be an effective analysis tool to evaluate the player's expected performance in each scenario. For example, the log can be used to compare a player who completes a scenario in one attempt and another player who completes the scenario in two attempts. Currently however, this analysis is performed manually using a log display tool that offers basic event filtering. The log analysis tool could be extended to provide automated summary comparisons between different scenario sessions.

3. Replay Feature

One new possible feature is a replay function, which could allow players to replay a scenario and watch the victories or mistakes made by other players. Players could pause and look at the detailed information during the replay. It could be useful for training and information dissemination. The replaying of scenarios could be based on the data log, and this would allow players to better understand their weaknesses.

4. Artificial Log File

In the real world, adjustment of firewall filtering rules is constantly carried out after the analysis of log files. In order to make CyberCIEGE scenarios more closely parallel the real world, an artificial firewall log file can be created to display a summary of the firewall traffic either graphically or as a text representation. The player would then analyze this log file and deploy his or her strategies accordingly. For example, when there is internal IP spoofing in the network, the log file may provide an indication of evidence that spoofing was attempted. When the firewall is successfully configured to deny IP spoofing, the recorded incidence of IP spoofing can be removed from the firewall log. In that way, players are reminded that they have to regularly monitor their log files to stay current with ongoing threats.

5. User Trial

A final recommendation would be to have all three filtering scenario tested with game players, i.e. students in an introductory computer security course, to see if the desired imparting of knowledge is actually achieved.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] Cynthia E. Irvine, Michael F. Thompson, Ken Allen. *An Information Assurance Teaching Tool for Training and Awareness.*

[2] The NPSPIN Group, Inc. *Peer to Peer Vs. Client/Server Networks.* Accessed on September 2005. URL: http://freepctech.com/pc/002/networks007.shtml

[3] Alan McLaughlin, Cypress Semiconductor. *Addressing Next-Gen Firewall Design Challenges Part I: Firewall Basic And Static Firewalls.* Retrieved on October 2005. URL: http://www.analogzone.com/iot_0516.pdf

[4] Carnegie Mellon University. *Home Computer Security.* Accessed on August 2005. URL : http://www.cert.org/homeusers/HomeComputerSecurity/glossary.html

[5] David W Chadwick, University of Salford. *Network Firewall Technologies.* Retrieved on September 2005. URL: http://sec.isi.salford.ac.uk/download/Firewalls.PDF

[6] *TCP/IP.* Accessed on June 2005. URL: http://www.webopedia.com/TERM/T/TCP_IP.html

[7] Microsoft TechNet. *Firewall.* Accessed on July 2005. URL: http://www.microsoft.com/technet/security/topics/networksecurity/firewall.mspx

[8] Gerhard Cronje. *Choosing The Best Firewall Version 1.2b.* Retrieved on September 2005. URL: http://securitytechnet.com/resource/security/firewall/951.pdf

[9] MOREnet Technical Support. *An Introduction to Network Firewalls and Firewall Selection Process.* Accessed on October 2005. URL: http://www.more.net/technical/netserv/tcpip/firewalls/

[10] D. Brent Chapman, Great Circle. *Network (In) Security Through IP Packet Filtering.* Accessed on September 2005. URL: http://www.greatcircle.com/pkt_filtering.html

[11] NIST. *Guidelines on Firewalls and Firewall Policy.* Retrieved on August 2005. URL: http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

[12] Ken Brown. *Network Security-Firewall.* Accessed on September 2005. URL: *http://www.bbk.ac.uk/ccs/news/newsletters/autumn02/firewall.htm*

[13] NIST. *Guide to Selecting Information Technology Security Products.* Retrieved on October 2005. URL: http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf

[14] *Scenarios*. Accessed on July 2005. URL: http://cisr.nps.navy.mil/cyberciege/ENCYLO/Scenarios.html

[15] *CyberCIEGE Game Scenarios*. Accessed on July 2005. URL: http://cisr.nps.navy.mil/cyberciege/ENCYLO/GameScenarios.html

[16] Koen Noens. Firewalls. Accessed on October 2005. URL: http://users.pandora.be/mydotcom/library/security/firewall.htm June, 2002.

[17] Tiat Leng, Teo. December 2003. *Scenarios Selection And Student Assessment Modules for CyberCIEGE.* Retrieved on July 2005. URL: http://cisr.nps.navy.mil/downloads/theses/03thesis_teo.pdf

[18] 2004 Rivermind, Inc. December 28, 2004 Version 15g. *Scenario Format Template*.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Ken Allen
   Rivermind, Inc
   Mountain View, California

4. Hugo A. Badillo
   NSA
   Fort Meade, Maryland

5. George Bieber
   OSD
   Washington, D.C.

6. RADM Joseph Burns
   Fort George Meade, Maryland

7. John Campbell
   National Security Agency
   Fort Meade, Maryland

8. Deborah Cooper
   DC Associates, LLC
   Roslyn, Virginia

9. CDR Daniel L. Currie
   PMW 161
   San Diego, California

10. Louise Davidson
    National Geospatial Agency
    Bethesda, Maryland

11. Vincent J. DiMaria
    National Security Agency
    Fort Meade, Maryland

12. Scott Gallardo
Rivermind, Inc
Mountain View, California

13. Jennifer Guild
SPAWAR
Charleston, South Carolina

14. Richard Hale
DISA
Falls Church, Virginia

15. LCDR Scott D. Heller
SPAWAR
San Diego, California

16. Wiley Jones
OSD
Washington, D.C.

17. Russell Jones
N641
Arlington, Virginia

18. Steve LaFountain
NSA
Fort Meade, Maryland

19. Dr. Greg Larson
IDA
Alexandria, Virginia

20. Gilman Louie
In-Q-Tel
Menlo Park, California

21. Ernest Lucier
Federal Aviation Administration
Washington, D.C.

22. CAPT Deborah McGhee
Headquarters U.S. Navy
Arlington, Virginia

23. Dr. Vic Maconachy
NSA
Fort Meade, Maryland

24. Doug Maughan
Department of Homeland Security
Washington, D.C.

25. Dr. John Monastra
Aerospace Corporation
Chantilly, Virginia

26. John Mildner
SPAWAR
Charleston, South Carolina

27. Jim Roberts
Central Intelligence Agency
Reston, Virginia

28. Keith Schwalm
Good Harbor Consulting, LLC
Washington, D.C.

29. Dr. Ralph Wachter
ONR
Arlington, Virginia

30. David Wennergren
DoN CIO
Arlington, Virginia

31. David Wirth
N641
Arlington, Virginia

32. Daniel Wolf
NSA
Fort Meade, Maryland

33. Jim Yerovi
NRO
Chantilly, Virginia

34. Dr. Cynthia E. Irvine
Naval Postgraduate School
Monterey, California

35. Paul C. Clark
Naval Postgraduate School
Monterey, California

36. Michael Thompson
Naval Postgraduate School
Monterey, California

37. Professor YEO Tat Soon
Director of Temasek Defence Systems Institute
National University of Singapore, Singapore

38. Ms Tan Lai Poh
Senior Admin. Officer of TDSI
National University of Singapore, Singapore

39. Nai Kwan, Tan
Student, Naval Postgraduate School
Monterey, California